



# Asante

A Communication Division of UIC Corporation



## IntraCore<sup>®</sup> 3724PWR

24-Port FastEthernet/12Ports PoE + 2 Gigabit Combo  
L2+ Management Switch

**User's Manual**



## IntraCore 3724PWR

24-Port FastEthernet/12 Ports PoE + 2 Gigabit Combo  
L2+ Management Switch

### User's Manual

Asante  
47709 Fremont Blvd  
Fremont, CA 94538  
USA

#### **SALES**

408-435-8388

#### **TECHNICAL SUPPORT**

408-435-8388: Worldwide

[www.asante.com/support](http://www.asante.com/support)  
support@asante.com

Copyright © 2008 Asante. All rights reserved. No part of this document, or any associated artwork, product design, or design concept may be copied or reproduced in whole or in part by any means without the express written consent of Asante. Asante and IntraCore are registered trademarks and the Asante logo, AsanteCare, Auto-Uplink, and IntraCare are trademarks of Asante. All other brand names or product names are trademarks or registered trademarks of their respective holders. All features and specifications are subject to change without prior notice.  
Draft D 9/18/08

## Table of Contents

IntraCore 3724PWR .....	2
Chapter 1 Introduction.....	7
1.1 Features.....	7
1.2 System Defaults.....	8
1.3 Package Contents.....	11
1.4 Front and Back Panel Descriptions.....	11
1.4.1 LEDs.....	13
1.5 Management and Configuration.....	13
1.5.1 Console Interface.....	13
Chapter 2: Hardware Installation and Setup .....	14
2.1 Installation Overview.....	14
2.1.1 Safety Overview.....	14
2.1.2 Recommended Installation Tools.....	15
2.1.3 Power Requirements.....	15
2.1.4 Environmental Requirements.....	15
2.1.5 Cooling and Airflow.....	15
2.2 Installing into an Equipment Rack.....	15
2.2.1 Equipment Rack Guidelines.....	16
2.3 SFP Mini GBIC Ports .....	16
2.4 Connecting Power.....	17
2.5 Connecting to the Network.....	17
2.5.1 10/100/1000BaseT Ports Cabling Procedures.....	17
2.5.2 Gigabit Ethernet Ports Cabling Procedures .....	18
Chapter 3: Initial Software Setup.....	20
3.1 Connecting to a Console.....	20

3.2 Connecting to a PC .....	22
3.3 Username and Password .....	22
3.5 Restoring Factory Defaults .....	23
Chapter 4: Understanding the Command Line Interface (CLI) .....	24
4.1 User Top (User EXEC) Mode .....	24
4.2 Privileged Top (Privileged EXEC) Mode .....	25
4.3 Global Configuration Mode .....	27
4.3.1 Interface Configuration Mode .....	28
4.4 Advanced Features Supported within the Command Mode .....	29
4.5 Using CLI Command History .....	31
4.6 Using Command-Line Editing Features and Shortcuts .....	32
4.6.1 Moving Around on the Command Line .....	32
4.6.2 Completing a Partial Command Name .....	33
4.6.3 Deleting Entries .....	33
Chapter 5: Managing the System and Configuration Files .....	34
5.1 Managing the System .....	34
5.1.1 Setting the System Clock .....	34
5.1.2 Specify the Hostname .....	35
5.1.5 Test Connections with Ping Tests .....	35
5.1.3 Enable the System Log .....	35
5.1.4 Displaying the Operating Configuration .....	35
5.2 Managing Configuration Files .....	36
5.2.1 Configuring from the Terminal .....	36
5.2.2 Copying Configuration Files to a Network Server .....	36
5.2.3 Copying Configuration Files from a Network Server to the Switch .....	37
5.3 Managing system image Files .....	38
5.3.1 Saving System image to a Network Server .....	38
5.3.2 Replacing System image from a Network Server .....	38
5.4 Configuring SNMP .....	38
5.4.1 Configuring SNMP Support .....	39

5.5 Spanning Tree Algorithm .....	40
5.5.1 Spanning Tree Parameters .....	40
5.5.2 Rapid Spanning Tree Protocol (RSTP) .....	41
5.5.3 Configuring spanning-tree .....	42
Chapter 6: Configuring IP .....	46
6.1 Establish Address Resolution .....	47
6.2 Managing IP Multicast Traffic .....	48
6.2.1 IGMP Overview .....	48
6.2.2 Configuring IGMP .....	48
6.3 Access Lists .....	50
6.3.1 Creating an Access List .....	50
6.3.2 Configuring an Access List .....	50
6.3.3 Applying an Access List to an Interface .....	52
6.3.4 Enabling an Access List .....	52
Chapter 7: Power over Ethernet (PoE) .....	53
7.1 PoE Definitions .....	53
7.2 PoE Show Example .....	55
7.2 PoE Interface Settings Example .....	57
Chapter 8: VLAN Configuration .....	58
8.1 Creating or Modifying a VLAN .....	58
8.2 VLAN Port Membership .....	59
8.2.1 configuring vlan ports .....	59
8.2.2 Trunk (IEEE 802.1q) .....	60
Chapter 9: Quality of Service Configuration .....	60
9.1 Scheduling algorithm .....	62
9.1.1 Configuring Weighted Round Robin .....	62
9.1.2 Monitoring Weighted Round Robin .....	63
9.2 Priority Queuing .....	63

9.2.1 Priority Mapping .....	63
9.2.2 Port Based QOS .....	64
9.2.3 802.1P Based QOS.....	64
9.2.4 IP Based QOS .....	64
9.3 Traffic Shaping.....	65
9.3.1 Configuring Traffic Shaping for an Interface.....	65
9.4 Rate Limiting .....	65
Chapter 10: Configuring the Switch Using the GUI .....	66
10.1 Main Configuration Menu .....	67
10.2 System .....	68
10.3 Ports .....	72
10.3.1 Power over Ethernet (PoE) .....	77
Chapter 11: CLI Commands .....	118
Appendix A: Basic Troubleshooting .....	148
Appendix B: Specifications .....	148
Appendix C: FCC Compliance and Warranty Statements.....	150
C.1 FCC Compliance Statement.....	150
C.2 Important Safety Instructions.....	150
C.3 IntraCore Warranty Statement.....	151
Index .....	152

# Chapter 1: Power over Ethernet (PoE)

The IntraCore IC3724PWR 24-port + 2 Gigabit Layer 2+ Managed Switch is a high-performance network switch used to reduce network congestion and application response times. The 24-port IntraCore IC3724PWR multi-protocol switch supports Layer 2+ and Ethernet switching. The switch has 24 10/100BaseT ports with Auto-Uplink and has 2 combination ports used for sharing with SFP mini GBICs. Fiber technology is used to connect two switches together. The switches also have an SNMP-based management agent embedded on the main board. This agent supports both in-band and out-of-band access for managing the switch.

These switches have a broad range of features for Layer 2+ switching delivering reliability and consistent performance for network traffic. The switches improve network performance by segregating them into separate broadcast domains with IEEE 802.1Q compliant VLANs and provide multimedia applications with multicast switching and CoS services.

The system can operate as a stand-alone network or be used in combination with other IntraCore switches in the backbone.

## 1.1 Features

The IntraCore IC3724PWR Ethernet switch is a 24-port Layer 2+ multi-media, multi-protocol (Ethernet and Layer 2+) switch. The following is a list of features:

- 24 port 10/100 switch with auto-uplink
- 2 port gigabit combo ports
- Supports wire-speed L2+ switching
- CoS provisioning on Layers 2 and 802.1p, IP precedence (TOS, DSCP )
- Packet filtering
- 8K MAC address
- Up to 255 configurable 802.1Q based VLAN groups
- Up to 256 multicast groups, statically created or dynamically created by IGMP snooping
- SNMP v1, v2, and RMON, statistics counters supported
- Spanning Tree Protocol 802.1D (standard), 32 instances of 802.1w (rapid) VLAN and 802.1s (multiple)
- 6 trunks and 8 ports/trunk link aggregation
- 4 MB internal packet buffer
- Support for Jumbo Frames (up to 9 KB in length)

## 1.2 System Defaults

The system defaults are the configuration parameters set in the factory. Use command 'Clear config' to restore the defaults followed by a 'save' command.

The following table lists some of the basic system defaults.

Function	Parameter	Default
Console Port Connection	Baud Rate	Auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	300 seconds
Authentication	login	Username "admin" Password "Asante"
	Enable Privileged Exec from Normal Exec Level	Username "admin" Password "Asante"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1x Port Authentication	Disabled
	HTTPS	Disabled
	Port Security	Disabled
IP Filtering	Disabled	
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Port Number	443
SNMP	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled



	<p>Flow Control</p> <p>Port Capability</p>	<p>Disabled</p> <p><b>1000BASE-T –</b></p> <p>10 Mbps half duplex  10 Mbps full duplex  100 Mbps half duplex  100 Mbps full duplex  1000 Mbps full duplex  Full-duplex flow control disabled  Symmetric flow control disabled</p> <p><b>1000BASE-SX/LX/LH –</b></p> <p>1000 Mbps full duplex  Full-duplex flow control disabled  Symmetric flow control disabled</p>
POE ports configuration	<p>Admin Status</p> <p>Power Management Mode</p> <p>Power Allocation</p> <p>Detection Type</p>	<p>Enabled</p> <p>Dynamic without priority</p> <p>15400 miliwatts</p> <p>IEEE 802.3af 4-Point Detection only</p>
Rate Limiting	Input and Output Limits	Disabled
Port Trucking	LACP (all ports)	Disabled
Broadcast Storm Protection	<p>Status</p> <p>Broadcast Limit Rate</p>	<p>Enabled (all ports)</p> <p>500 packets per second</p>
Spanning Tree Protocol	Status	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	<p>Default VLAN</p> <p>PVID</p> <p>Acceptable Frame Type</p> <p>Ingress Filtering</p> <p>Switchport Mode (egress mode)</p>	<p>1</p> <p>1</p> <p>All</p> <p>Disabled</p> <p>untagged frames</p>

Traffic Prioritization	Ingress Port Priority Weighted Round Robin IP Precedence Priority IP DSCP Priority	0 Queue: 1 2 3 4 Weight: 1 2 4 8 Disabled Disabled
IP Settings	IP Address Subnet Mask Default Gateway DHCP ARP	192.168.0.1 255.255.255.0 0.0.0.0 Client: Disabled Enabled
Multicast Filtering	IGMP Snooping	Disabled
System Log	Remote logging Memory-log Flash-log	Disabled Enabled Enabled
SNTP	Clock Synchronization	Disabled

## 1.3 Package Contents

The following items are included in the switch's package:

- Switch
- AC power cord
- RS232 straight-through serial cable for management console port
- Rack mount brackets with screws
- IntraCore IC3724PWR CD-ROM

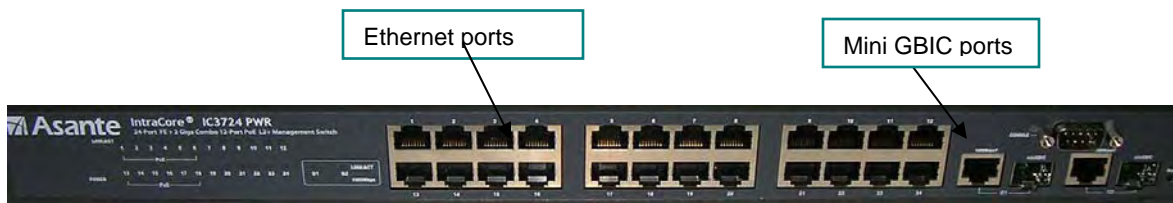
Contact your dealer immediately if any of these items is missing.

## 1.4 Front and Back Panel Descriptions

The following section describes the front and back panels of the IntraCore IC3724PWR Series switches.

The front panel of the IntraCore IC3724PWR contains the following: power and port LEDs, 24 10/100BaseT ports, and 2 dual-function Gigabit ports that support either 1000BaseT or mini GBIC Gigabit Ethernet ports. The console port may be front or back depending on model. For information on LEDs refer to the following section in this chapter.

### 3724PWR Front Panel



### 3724PWR Rear Panel





### 1.4.1 LEDs

The IC3724PWR front panel LED display allows you to monitor the status of the switch.

The IC3724PWR has one power LED indicator. There are also LED indicators for each of the ports. Refer to the following table for LED information.

LED	Color	Description
Power	Green	Power is on.
	Off	Power is off, or main power has failed.
1000Mbps	Amber	A valid 1000 Mbps link has been established on the port.
	Off	No link has been established on the port or if Link/Activity led is on, the speed is either 100 or 10 Mbps.
POE	Amber	A POE device is connected to the port and drawing power.
	Off	No POE device is connected to the port, no power is being drawn.
Link/Activity	Green	A link has been established on the port.
	Blinking Green	Activity has been detected.
	Off	No link has been established on the port.

## 1.5 Management and Configuration

The switch is managed using Command Line Interface (CLI) in order to access several different command modes. Entering a question mark (?) at each command mode's prompt provides a list of commands.

### 1.5.1 Console Interface

Support for local, out-of-band management is delivered through a terminal or modem attached to the EIA/TIA-232 interface. You can access the switch by connecting a PC or terminal to the console port of the switch, via a serial cable. The default username/ password set on the console line is admin/**Asante** (it is case-sensitive). The default IP address is **192.168.0.1**. It can be modified to suit your network setup. See 3.4 for details.

Remote in-band management is available through Simple Network Management Protocol (SNMP) and Telnet client. When connecting via a Telnet session, the default login/password is also **admin/Asante** (case-sensitive).

See Chapter 2 for more information on connecting to the switch.

## Chapter 2: Hardware Installation and Setup

Use the following guidelines to easily install the switch, ensuring that it has the proper power supply and environment.

### 2.1 Installation Overview

Follow these steps to install the IntraCore IC3724PWR switch:

1. Open the box and check the contents. See *Chapter 1.2 Package Contents* for a complete list of the items included with the IntraCore IC3724PWR switch.
2. Install the switch in an equipment or wall rack, or prepare it for desktop placement.
3. Connect the power cord to the switch and to an appropriate power source.
4. Connect network devices to the switch.

See the sections below for more detailed installation instructions.

#### 2.1.1 Safety Overview

The following information provides safety guidelines to ensure your safety and to protect the switch from damage.

**Note:** This information is a guideline, and may not include every possible hazard. Use caution when installing this switch.

- Only trained and qualified personnel should be allowed to install or replace this equipment
- Always use caution when lifting heavy equipment
- Keep the switch clean
- Keep tools and components off the floor and away from foot traffic
- Avoid wearing rings or chains (or other jewelry) that can get caught in the switch. Metal objects can heat up and cause serious injury to persons and damage to the equipment.
- Avoid wearing loose clothing (such as ties or loose sleeves) when working around the switch

When working with electricity, follow these guidelines:

- Disconnect all external cables before installing or removing the cover
- Do not work alone when working with electricity
- Always check that the cord has been disconnected from the outlet before performing hardware configuration

- Do not tamper with the equipment. Doing so could void the warranty
- Examine the work area for potential hazards (such as wet floors or ungrounded cables)

### 2.1.2 Recommended Installation Tools

You need the following additional tools and equipment to install the switch into an equipment rack:

- Flat head screwdriver
- Phillips head screwdriver
- Antistatic mat or foam

### 2.1.3 Power Requirements

The electrical outlet should be properly grounded, located near the switch and be easily accessible. Make sure the power source adheres to the following guidelines:

- Power: Auto Switching AC, 90-240 VAC
- Frequency range: 50/60 Hz

### 2.1.4 Environmental Requirements

Install the switch in a clean, dry, dust-free area with adequate air circulation to maintain the following environmental limits:

- Operating Temperature: 0° to 40°C (32° to 104°F)
- Relative Humidity: 5% to 95% non-condensing

Avoid direct sunlight, heat sources, or areas with high levels of electromagnetic interference. Failure to observe these limits may cause damage to the switch and void the warranty.

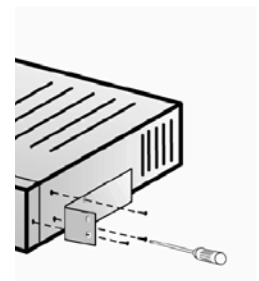
### 2.1.5 Cooling and Airflow

The IntraCore IC3724PWR switch uses internal fans for air-cooling. Do not restrict airflow by covering or obstructing air vents on the sides of the switch.

## 2.2 Installing into an Equipment Rack

**Important:** Before continuing, disconnect all cables from the switch.

To mount the switch into an equipment rack:



1. Place the switch on a flat, stable surface.
2. Locate a rack-mounting bracket (supplied) and place it over the mounting holes on one side of the switch.
3. Use the screws (supplied) to secure the bracket (with a Phillips screwdriver).
4. Repeat the two previous steps on the other side of the switch.
5. Place the switch in the equipment rack.
6. Secure the switch by securing its mounting brackets onto the equipment rack with the appropriate screws (supplied).

**Important:** Make sure the switch is supported until all the mounting screws for each bracket are secured to the equipment rack. Failure to do so could cause the switch to fall, which may result in personal injury or damage to the switch.

### 2.2.1 Equipment Rack Guidelines

Use the following guidelines to ensure that the switch will fit safely within the equipment rack:

- Size: 17.5 x 12.7 x 1.8 inches (440 x 234 x 45 mm)
- Ventilation: Ensure that the rack is installed in a room in which the temperature remains below 104° F (40° C). Be sure that no obstructions, such as other equipment or cables, block airflow to or from the vents of the switch
- Clearance: In addition to providing clearance for ventilation, ensure that adequate clearance for servicing the switch from the front exists

## 2.3 SFP Mini GBIC Ports

The GBIC Interface is the industry standard for Gigabit Ethernet Interfaces.

The Gigabit SFP module inserts into the Mini GBIC port to create a new Gigabit port. The hot-swapping feature on the IntraCore IC3724PWR lets you install and replace the SFP transceivers while the system is operating; you do not need to disable the software or shut down the system power.

To install the module, do the following:

1. Insert the transceiver with the optical connector facing outward and the slot connector facing down. The module is keyed to help establish the correct position.
2. Slide the SFP transceiver into the slot until it clicks into place.
3. Remove the module's rubber port cap.
4. Connect the cable to the Gigabit SFP module's port.

**Caution:** When replacing a SFP transceiver you must always disconnect the network cable before removing a transceiver.



## 2.4 Connecting Power

**Important:** Carefully review the power requirements (Chapter 2.1.3) before connecting power to the switch.

Use the following procedure to connect power to the switch:

- Plug one end of the supplied power cord into the power connector on the back of the switch.
- Plug the other end into a grounded AC outlet.

The power LED show the initialization is in process. The front panel LEDs blink and the power LED illuminates when it has initialized. The switch is ready for connection to the network.

**Important:** If the power does not come on, check the next section to ensure that the correct cabling is used.

## 2.5 Connecting to the Network

The switch can connect to an Ethernet network with the switch turned on or off. Use the following procedure to make the network connections:

- Connect the network devices to the switch, following the cable guidelines outlined below.
- After the switch is connected to the network, it can be configured for management capabilities (see the following chapters for information on configuration).

### 2.5.1 10/100/1000BaseT Ports Cabling Procedures

The 10/100/1000 ports on the switch allow for the connection of 10BaseT, 100BaseTX, or 1000BaseT network devices. The ports are compatible with IEEE 802.3 and 802.3u standards.

**Important:** The switch must be located within 100 meters of its attached 10BaseT or 100BaseTX devices.

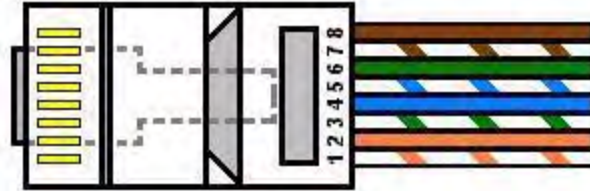
Use the following guidelines to determine the cabling requirements for the network devices:

- Connecting to Network Station: Category 5 UTP (Unshielded Twisted-Pair) straight-through cable (100 m maximum) with RJ-45 connectors
- Connecting to Repeater/Hub/Switch's Uplink port: Category 5, UTP straight-through cable (100 m maximum) with RJ-45 connectors

**Note:** These switches have no specific uplink ports. All 10/100/1000 ports on these switches are auto-sensing MDI/MDI-X. This advanced feature means that when the ports are operating at 10/100Mbps, they will automatically

determine whether the device at the other end of the link is a hub, switch, or workstation, and adjust its signals accordingly. No crossover cables are required.

Although 10/100BaseT requires only pins 1, 2, 3, and 6, you should use cables with all eight wires connected as shown in Table 2-2 below.



1000BaseT requires that all four pairs (8 wires) be connected correctly, using Category 5 or better Unshielded Twisted Pair (UTP) cable (to a distance of 100 meters). Table 2-2 shows the correct pairing of all eight wires.

Pin Number	Pair Number & Wire Colors
1	2 White / Orange
2	2 Orange / White
3	3 White / Green
4	1 Blue / White
5	1 White / Blue
6	3 Green / White
7	4 White / Brown
8	4 Brown / White

## 2.5.2 Gigabit Ethernet Ports Cabling Procedures

Cabling requirements for the optional hardware modules depend on the type of module installed. Use the following guidelines to determine the particular cabling requirements of the module(s):

- 1000BaseSX GBIC: Cables with SC-type fiber connectors; 62.5 $\mu$  multi-mode fiber (MMF) media up to 275 m (902'), or 50 $\mu$  MMF media up to 550 m (1805')
- 1000BaseLX GBIC: Cables with SC-type fiber connectors; 10 $\mu$  single-mode fiber media up to 5 km (16,405')
- 1000BaseLH GBIC: Cables with SC-type fiber connectors; 10 $\mu$  single-mode fiber media up to 20 km (65,617')
- 1000BaseLX Long Haul GBIC: Cables with SC-type fiber connectors; 10 $\mu$  single-mode fiber media up to 100 km (328,100')

- 1000BaseLZ GBIC: Cables with SC-type fiber connectors; 10 $\mu$  single-mode fiber media up to 120 km (393,701')
- 1000BaseT: Category 5 or better Unshielded Twisted Pair (UTP) cable up to 100 m (328.1')

When attaching a workstation to the switch, a standard straight-through CAT5 cable may be used, even when the workstation is attached via a patch panel. No crossover cable is needed with the MDX/MDI ports. The switch should be kept off the network until proper IP settings have been set.

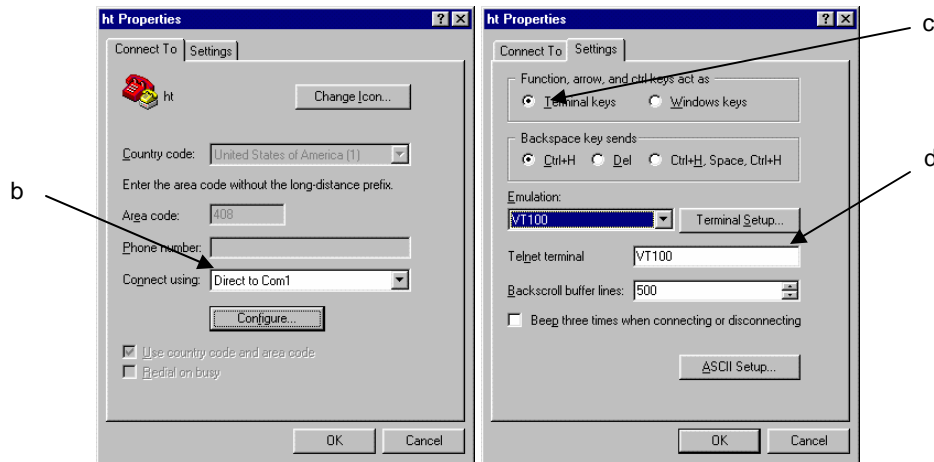
## Chapter 3: Initial Software Setup

Configure the switch by connecting directly to it through a console (out-of-band management), running a terminal emulation program, such as HyperTerminal or by using telnet.

### 3.1 Connecting to a Console

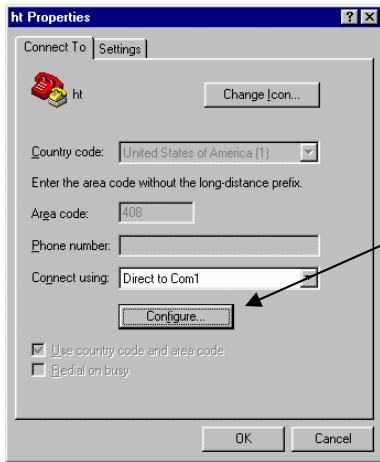
To connect the switch to a console or computer, set up the system in the following manner:

7. Plug power cord into the back of the switch.
8. Attach a straight-through serial cable between the RS232 console port and a COM port on the PC.
9. Set up a HyperTerminal (or equivalent terminal program) in the following manner:
  - a. Open the HyperTerminal program, and from its file menu, right-click on **Properties**.
  - b. Under the **Connect To** tab, choose the appropriate COM port (such as COM1 or COM2).

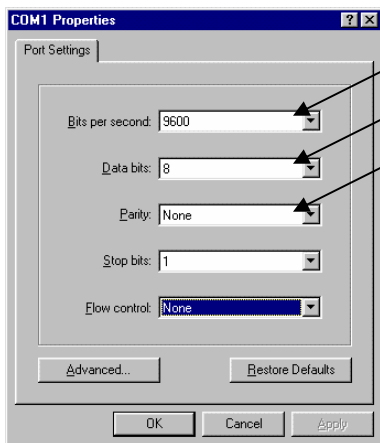


- c. Under the **Settings** tab, choose Select Terminal keys for Function, Arrow, and Ctrl keys. Be sure the setting is for Terminal keys, NOT Windows keys
- d. Choose VT100 for Emulation mode.

- e. Press the **Configuration** button from the Connect To window.



- f. Set the data rate to 9600 Baud.
- g. Set data format to 8 data bits, 1 stop bit and no parity.
- h. Set flow control to NONE.



Now that terminal is set up correctly, power on the switch. The boot sequence will display in the terminal.

After connecting to the console, you will be asked for a password

The initial default password for access using either the console or telnet is Asante (case-sensitive). Refer to the following section for setting passwords on the terminal lines.

## 3.2 Connecting to a PC

You can connect to the switch through a PC by using either an Ethernet or USB cable. Using a telnet session, you can telnet into the switch. The default IP address is 192.168.0.1. The case-sensitive default password is Asante.

## 3.3 Username and Password

The default Username/Password is admin/Asante.

## 3.4 Configuring an IP Address

The switch ships with the default IP address **192.168.0.1/255.255.255.0**. Connect through the serial port in order to assign the switch an IP address on your network.

The physical ports (or switchports) of the IntraCore 3724PWR are L2 ports, and cannot have an IP address assigned to them. By default, each switchport belongs to VLAN 1. Use the following instructions to configure an IP address to the switch. Follow the steps below to change the switch's IP address.

1. Connect to the console and Enter at the Username prompt the username and password as described above.
2. The screen displays the user mode prompt, `COMMAND>`.
3. Type **enable**. Enter username and password. The new prompt is `Switch#`.
4. Type **configuration**. The new prompt is `Switch(config)#`.
5. Type `network parms <ip address> <subnet mask> <default gateway>`

```
Switch# configuration
Switch(config)# network parms 192.168.0.10 255.255.255.0 192.168.0.254
Switch(config)# exit
Switch# save
Switch# show network
    MAC Address: 00-03-6d-ff-ef-4c
    Management VLAN: 1
    STATIC
    IP: 192.168.0.10
    Netmask: 255.255.255.0
    Gateway: 192.168.0.254
```

### 3.5 Restoring Factory Defaults

To restore the switch to its factory default settings, follow the commands shown in the following screen.

```
COMMAND> enable
Switch# clear config
Switch# save
```

**Important:** To retain configuration changes after a system reload you must save changes made in running configuration. From the privileged level, configurations can be saved using the **save** command.

The switch is ready for configuration. Refer to the following chapters for management and configuration information.

## Chapter 4: Understanding the Command Line Interface (CLI)

The switch utilizes Command Line Interface (CLI) to provide access to several different command modes. Each command mode provides a group of related commands. In general, after typing a command name, always press 'enter' to start the execution of the command.

After logging into the system, you are automatically in the *user top (user EXEC) mode*. From the user top mode you can enter into the *privileged top (privileged EXEC) mode*. From the privileged EXEC level, you can access the global configuration mode and specific configuration modes: interface and Switch configuration. Entering a question mark (?) at the system prompt provides a list of commands available for each command mode.

### Document Conventions

Command descriptions use the following conventions:

- Vertical bars ( | ) separate alternative, mutually exclusive, elements
- Braces ( { } ) indicate a required choice
- **Boldface** indicates commands and keywords that are entered literally as shown
- *Italics* indicate arguments for which you supply values

### Access Each Command Mode

The following sections describe how to access each of the CLI command modes:

- User Top Mode: COMMAND>
- Privileged Top Mode: Switch#
  - Global Configuration Mode: Switch(config)#
  - Interface Configuration Mode: Switch(interface #)#

### 4.1 User Top (User EXEC) Mode

After you log in to the Switch, you are automatically in user top (user EXEC) command mode. The user-level prompt consists of the 'COMMAND' followed by the angle bracket (>):



```
COMMAND>
```

The user top commands available at the user level are a subset of those available at the privileged level. In general, the user top commands allow you ping remote hosts and show port statistics.

To list the commands available in user top mode, enter a question mark (?). Use a space and a question mark (?) after entering a command to see all the options for that particular command.

Command	Purpose
?	Lists the user EXEC commands.
show ?	Lists all the options available for the given command.

User top commands:

```
COMMAND> ?
Help           Displays Help information
?              Displays Help information
logout         Exit
ping           Pings a remote host
show           Display commands
enable        Enter XCLI interface
```

You may also enter a question mark after a letter or string of letters to view all the commands that start with that letter (with no space between the letter and the question mark). Please note that there is no help on the arguments after a command is typed.

Use 'logout' to logout from the switch.

## 4.2 Privileged Top (Privileged EXEC) Mode

Because many of the privileged commands set the system configuration parameters, privileged access can be password protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which you can access the remaining command modes. The following example shows how to access privileged EXEC mode. Notice the prompt changes from `COMMAND>` to `Switch#`:

To execute a command, the command and its arguments or key words must be entered in their entirety. However, a partially typed command, argument or key word can be completed by pressing the 'tab' key.

```
COMMAND> enable
Username : admin
Password : xxxxxx
Switch#
```

Command	Purpose
COMMAND> <b>enable</b>	Enters the privileged EXEC mode.
Switch# ?	Lists privileged EXEC commands.

To return to user EXEC mode, use the **exit** command.

To list the commands available in top mode, enter a question mark (?) at the prompt, as shown in the following example. Enter a question mark (?) after a command to see all the options for that command.

```
Switch> enable
Switch# ?
```

```
cable-diag      Proceed cable diagnostic
clear           Command to clear switch configuration or statistics
configuration   Enter into global configuration mode
copy            Upload file from switch to host, or download file to
                switch from host
exit            Exit current shell
help            Displays Help information
logout          Exit current shell
ping            Proceed ping destination host
reload          Reboot System
save            Save configuration
show            Show configured data
telnet          Telnet the other host
```

**Important:** To retain configuration changes after a system reload you must save changes made in running configuration. From the privileged level, configurations can be saved using the **save** command.

### 4.3 Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just one protocol or interface. Commands to enable a particular routing function are also global configuration commands. To enter the global configuration mode, use the **configure** command.

The following example shows how to access and exit global configuration mode and list global configuration commands.

Command	Purpose
Switch# <b>configuration</b>	From privileged EXEC mode, enters global configuration mode.
Switch(config)# ?	Lists the global configuration commands.

To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands:

Command	Purpose
<b>exit</b>	Exits global configuration mode and returns to privileged EXEC mode.

To list the commands available in global configuration mode, enter a question mark (?) at the prompt, as shown in the following example. Enter a question mark (?) after a specific command to see all the options for that command.

```
Switch(Config)# ?
  exit                Exit current shell
  link-aggregation    Configure link aggregation
  vlan                Configure VLAN
  arp                 Configure ARP functions
  access-list         Configure Access-list
  bridge              Configure switch aging time
  dos                 Configure denial of service
  lacp-syspri         Configure LACP system priority
  lldp                Configure LLDP
```

log	Configure log server
radius-server	Configure radius server
static-address	Static address
mgmt-accesslist	Set management access list, allows up to 8 IP addresses
monitor	Configure port mirroring
dot1x	Configure 802.1x parameters
network	Configuration for inband connectivity
port-all	Configure all switch ports
qos	Configure QoS
rmon	Configure Remote Monitoring
set	Configure IGMP and static multicast
snmp	Configure SNMP parameters
sntp	Configure SNTP
https	Configure SSL
spanning-tree	Configure spanning-tree
tacplus	Configure tacacs+
user	Change user password
interface	Enter into configure interface mode
green-eth	Configure Green Ethernet enable or disable
Switch(Config)#	

From global configuration mode, you can access three additional configuration modes: Use the **interface** command to access its configuration modes.

### 4.3.1 Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type as Ethernet.

In the following example shows configuration of Ethernet interface 1. The new prompt, `Switch(interface 1)#`, indicates the interface configuration mode. In this example, the user asks for help by requesting a list of commands.

```

Switch(Config)# interface 1
Switch(Interface 1)# ?

  exit                Exit current shell
  dot1x               Configure 802.1x mode
  lacp                Configure port LACP mode
  addport             Add one port to a LAG group
  delport             Remove a port from a LAG group
  lldp                Configure lldp port level settings
  admin-mode          Configure administrative mode on a port
  auto-negotiate      Configure auto-negotiate mode on a port
  speed               Configure port phy parameter
  flow-control         Configure port flow control
  port-security        Configure port security
  qos                 Configure port-based QoS priority mapping
  rate-limit           Configure rate limit on a port
  storm-control        Configure storm control on a port
  rmon-counter         Configure RMON counter capability on a port
  set                  Configure an IGMP router port
  spanning-tree        Configure port spanning-tree
  vlan                 Configure VLAN properties on a port
  interface            Change to another interface

Switch(Interface 1)#

```

To exit interface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to top mode, use the **exit** command.

#### 4.4 Advanced Features Supported within the Command Mode

Enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also get a list of any command's associated keywords and arguments with the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, perform one of the following commands:

Command	Purpose
Help	Obtain a brief description of the help system in any command mode.
?	List all commands available for a particular command mode.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is word help, because it completes a word for you.

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the question mark (?). This form of help is command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

### Example of Context Sensitive Help

The following example illustrates how the context-sensitive help feature creates an access list from the configuration mode.

Enter the letters “co” at the system prompt followed by a question mark (?). Do not leave a space between the last letter and the question mark (?). The system provides the commands that begin with co.

```
Switch# co?
configuration  Enter configuration mode
copy          Copy from one file to another
Switch# co
```

Enter the **configure** command followed by a space and a question mark (?) to list the command’s keyword(s) and a brief explanation:

```
Switch# configure ?
<cr>
```

Note that in the example below, if you enter the ip command followed by the Return Key or Enter, the system returns the prompt that the command is incomplete.

```
Switch# copy
% Invalid command input
Switch#
```

Generally, uppercase letters represent variables. For example, after entering a command, such as **hostname**, and using a space and a question mark, you will be prompted for the new name, represented by **WORD**. In cases where an IP address is the variable, the uppercase letters **A.B.C.D** will represent it.

```
Switch(config)# network parms ?
A.B.C.D          Enter IP address of the switch
```

In the following access list example, seven further options are listed after the question mark. Note that what is typed so far is preserved after the display.

```
Switch(Config)# access-list name acl_1 ?

  add                Create a new access-list
  action             Specify the action of the ACL entry
  clear              Clear ACL entry contents
  delete             Remove the ACL entry
  enable             Enable the ACL entry
  disable            Disable the ACL entry
  set                Set ACL entry contents

Switch(Config)# access-list name acl_1
```

## 4.5 Using CLI Command History

The CLI user interface provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. To recall commands from the history buffer, use one of the following commands:

Keystrokes/Command	Purpose
Press the up arrow key	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press the down arrow key	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key

	sequence to recall successively more recent commands.
--	---

## 4.6 Using Command-Line Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the CLI command-line interface. The following subsections describe these features:

- Moving Around on the Command Line
- Completing a Partial Command Name
- Editing Command Lines that Wrap
- Deleting Entries
- Scrolling Down a Line or a Screen
- Redisplaying the Current Command Line
- Transposing Mistyped Characters
- Controlling Capitalization

### 4.6.1 Moving Around on the Command Line

Use the following keystrokes to move the cursor around on the command line in order to make corrections or changes:

Keystrokes	Purpose
Press the left arrow.	Move the cursor back one character.
Press the right arrow.	Move the cursor forward one character.

**Note:** The arrow keys function only on ANSI-compatible terminals such as VT100s.



## 4.6.2 Completing a Partial Command Name

If you cannot remember a complete command name, press the **Tab** key to allow the system to complete a partial entry.

Keystrokes	Purpose
Enter the first few letters and press <b>Tab</b> .	Complete a command name.

In the following example, when you enter the letters “conf” and press the **Tab** key, the system provides the complete command:

```
Router# conf<Tab>
Router# configuration
```

The command is not immediately executed, so that you may modify the command if necessary.

You may also enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter entered and the question mark (?). For example, two commands in privileged mode start with *co*. To see what they are, type **co?** at the privileged EXEC prompt:

```
Switch# co?
configuration copy
Switch# co
```

## 4.6.3 Deleting Entries

Use any of the following commands to delete command entries if you make a mistake or change your mind:

Keystrokes	Purpose
Press <b>Backspace</b> .	Erase the character to the left of the cursor.

## Chapter 5: Managing the System and Configuration Files

This chapter explains how to manage the system information, as well as how to manage the configuration files for IntraCore 3724PWR.

### 5.1 Managing the System

This section discusses the following tasks needed to manage the system information of the IntraCore 3724PWR:

- Setting the System Clock
- Configuring the Host name
- Changing the Password
- Testing Connections with Ping Commands
- Tracing Packet Routes
- Enabling Syslog
- Displaying the Operating Configuration

#### 5.1.1 Setting the System Clock

The IntraCore 3724PWR has a battery-backed system clock that is accurate even after a system restart.

To manually set the system clock, complete the following commands in privileged configuration mode. Use a space and a question mark (?) to display the clock set options. Save after configuring the clock by typing **save** at the switch# prompt.

```
Switch(Config)# sntp
    daylight          Enable or disable the daylight saving configuration
    localtime         Configure the local time
    server
    timezone

Switch(Config)# sntp localtime
    enable            Enable local time
    localtime_date    Set local time

Switch(Config)# sntp localtime localtime_date
    <2007..2037>      Enter year

Switch(Config)# sntp localtime localtime_date 2008 07 06 06 35 00

Switch(Config)#
```

### 5.1.2 Specify the Hostname

The factory-assigned default host name is **Switch**. To specify or modify the host name for the network, use the **Network sysinfo sysname** global configuration command.

Command	Purpose
<b>Network sysinfo sysname</b> <i>name</i>	This systems hostname.

### 5.1.5 Test Connections with Ping Tests

The switch supports IP ping, which can be used to test connectivity to remote hosts, via their IP addresses. Ping sends an echo request packet to an address and “listens” for a reply. The ping request will receive one of the following responses:

- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic
- Request timed out—There is no response, indicating a connection failure to the host, or the host has discarded the ping request

Beginning in user mode, use this command to ping another device on the network from the switch:

Command	Purpose
<b>ping</b> <i>address</i>	Send an ICMP echo message to a designated host for testing connectivity.

### 5.1.3 Enable the System Log

The IntraCore 3724PWR sends syslog messages to manager servers. Syslog messages are collected by a standard UNIX or NT type syslog daemon.

Syslog enables the administrator to centrally log and analyze configuration events and system error messages such as interface status, security alerts, environmental conditions, and CPU process overloads.

To log messages, use the following command in global configuration mode.

Command	Purpose
<b>log</b> <i>address</i>	IP address of the host to be used as a syslog server.
<b>log facility</b>	Facility parameters for syslog messages.
<b>log trap</b>	Set syslog server logging level.

### 5.1.4 Displaying the Operating Configuration

The configuration file may be displayed from the EXEC (enable) mode.

To see the current operating configuration, enter the following command at the enable prompt:

```
Switch# show running-config
```

## 5.2 Managing Configuration Files

This section discusses how to download configuration files from remote servers, and store configuration files on the switch at system startup.

Configuration files contain the commands the switch uses to customize the function of the IC3724PWR. The setup command facility helps you create a basic configuration file. However, you can manually change the configuration by typing commands in a configuration mode.

### 5.2.1 Configuring from the Terminal

The configuration files are stored in the following places:

- The running configuration is stored in RAM
- The startup configuration is stored in nonvolatile random-access memory (NVRAM)

To enter the configuration mode, enter the **configuration** command at the privileged EXEC prompt. The software accepts one configuration command per line. You can enter as many configuration commands as you want.

You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!).

### 5.2.2 Copying Configuration Files to a Network Server

You can copy configuration files from the switch to a file server using TFTP. You might wish to back up a current configuration file to a server before changing its contents, thereby allowing you to later restore the original configuration file from the server.

**Important:** TFTP is not a secure protocol. Your server IP address and configuration file name will not be protected over the public Internet. Use TFTP only on a trusted LAN connection.

To specify that the running or startup configuration file be stored on a TFTP network server, use the following commands in the EXEC mode.

The following is an example of copying the current configuration to a file called 'July' on server 192.168.123.100.

```
Switch# copy
  nvram_config      Backup switch configuration
  system_image     Backup switch runtime image
  tftp              Download configuration or runtime image from host to switch

Switch# copy nvram_config
  tftp              Specify tftp server

Switch# copy nvram_config tftp
  A.B.C.D           Enter tftp server IP address
```

```

Switch# copy nvram_config tftp 192.168.123.100
file                               Specify a filename

Switch# copy nvram_config tftp 192.168.123.100 file
WORD                               Enter filename for backup configuration

Switch# copy nvram_config tftp 192.168.123.100 file July
<cr>

Switch# copy nvram_config tftp 192.168.123.100 file July

Switch#

```

### 5.2.3 Copying Configuration Files from a Network Server to the Switch

You can copy configuration files from a TFTP server to the running configuration of the switch. You may want to do this for one of the following reasons:

To restore a previously backed up configuration file.

10. To use the same configuration file for another switch. For example, you may add another switch to your network and want it to have a similar configuration to the original switch. By copying the file to the new switch, you can change the relevant parts rather than re-creating the whole file.
11. To load the same configuration commands onto all the switches in your network so that they all have the same configurations.

The **copy nvram\_config** command loads the configuration files into the switch as if you were typing the commands in at the command line. The switch does not erase the existing running configuration before adding the commands unless a command in the copied configuration file replaces a command in the existing configuration file. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration may not be replaced or negated. In this case, the resulting configuration file will be a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To copy a configuration file from a TFTP server to the switch, use one of the following commands in EXEC mode:

Command	Purpose
<b>Switch# copy tftp 192.168.123.254 file cfg_file nvram_config</b>	Copy the config file 'cfg_file' from a TFTP server 192.168.123.254 to the switch.

To clear the saved configuration and restore configuration to default values, use the following command from privileged mode:

```
Switch# clear config
```

Don't forget to use **'save'** command to preserve the new configuration across reboots.

## 5.3 Managing system image Files

This system image file is stored in the non-volatile flash in the switch. It is the software that runs in the switch after power up. It provides user interfaces (CLI, Web, telnet) for user to control and manage the switch. The following describes the commands that save the system image to a file in a host TFTP server and download a new version system image from a TFTP server to the switch.

### 5.3.1 Saving System image to a Network Server

You can save the system image file of the switch to a file server using TFTP. You might wish to back up the current system image file to a server , thereby allowing you to later restore the original system image from the server in case of system image file corruption.

To save the system image file of the switch to a TFTP server, use one of the following commands in EXEC mode:

Command	Purpose
<code>copy system_image tftp 192.168.0.254 file ttt sysimg_file</code>	Copy the system image the file 'sysimg_file' to TFTP server 192.168.0.254.

### 5.3.2 Replacing System image from a Network Server

You can replace the system image file of the switch from a file in a server using TFTP. You can update the current system image with a newer version in this fashion.

To replace the system image file of the switch from a TFTP server, use one of the following commands in EXEC mode:

Command	Purpose
<code>copy tftp 192.168.0.254 file new_sysimg system_image</code>	Copy the system image the file 'new_sysimg' from TFTP server 192.168.0.254 to the switch.

## 5.4 Configuring SNMP

This section discusses the following tasks needed to configure Simple Network Management Protocol (SNMP).

### 5.4.1 Configuring SNMP Support

The Simple Network Management Protocol (SNMP) system consists of three parts: an SNMP manager, an SNMP agent, and a Management Information Base (MIB). SNMP is an application-layer protocol that allows SNMP manager and agent stations to communicate. SNMP provides a message format for sending information between an SNMP manager and an SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, the relationship between the manager and the agent must be defined.

The *SNMP agent* gathers data from the *MIB*, which holds the information about device parameters and network data. The agent also responds to the manager's requests to get or set data. An agent can also send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a specific event on the network. Such events include improper user authentication, restarts, link status (up or down), closing of a TCP connection, or loss of connection to a neighboring switch. An *SNMP manager* can request a value from an agent, or store or change a value in that agent.

To configure support for SNMP on the switch, perform the following tasks:

- Create an SNMP user group

Command	Purpose
<b>Switch(Config)# snmp group add read_grp version 1 access ro</b>	Create a 'read_only' version 1 group 'read_grp'

- Create an SNMP user of the group just created

Command	Purpose
<b>Switch(Config)# snmp user add user_read group read_grp version 1</b>	Create a version 1 user 'user_read' of group 'read_grp'

- Create a community string and management station

Command	Purpose
<b>snmp community add public group read_grp mgmt-ip 192.168.123.100</b>	Create a community string 'public' for group 'read_grp' that can be used by management host 192.168.123.100

- Define SNMP Trap Operations

Command	Purpose
<b>snmp trapstation add 192.168.123.100 community public type linkchange trap-version 1</b>	Create a trap host 192.168.123.100 to which the switch can send version 1 link change trap messages using community string 'public'.

## 5.5 Spanning Tree Algorithm

The Spanning Tree Protocol (STP) is part of the IEEE 802.1D standard. It provides for a redundant network without the redundant traffic through closed paths. For example, in a network without spanning tree protocol, the same message will be broadcast through multiple paths, which may start an unending packet-passing cycle. This in turn causes a great amount of extra network traffic, leading to network downtime. The STP reduces a network like this, with multiple, redundant connections, to one in which all points are connected, but where there is only one path between any two points (the connections span the entire network, and the paths are branched, like a tree).

All of the bridges (a switch is a complex bridge) on the network communicate with each other using special packets of data called Bridge Protocol Data Units (BPDUs). The information exchanged in the BPDUs allows the bridges on the network to do the following:

- Elect a single bridge to be the root bridge
- Calculate the shortest path from each bridge to the root bridge
- Select a designated bridge on each segment, which lies closest to the root and forwards all traffic to it
- Select a port on each bridge to forward traffic to the root
- Select the ports on each bridge that forward traffic, and place the redundant ports in blocking states

### 5.5.1 Spanning Tree Parameters

The operation of the spanning tree algorithm is governed by several parameters.

#### Forward Time

After a recalculation of the spanning tree, the Forward Time parameter regulates the delay before each port begins transmitting traffic. If a port begins forwarding traffic too soon (before a new root bridge has been selected), the network can be adversely affected. The default value for Forward Time is 15 seconds.

#### Hello Time

This is the time between BPDUs transmitted by each bridge. The default setting is 2 seconds.

#### Maximum Age



Each bridge should receive regular configuration BPDUs from the direction of the root bridge. If the maximum age timer expires before the bridge receives another BPDU, it assumes that a change in the topology has occurred, and it begins recalculating the spanning tree. The default setting for Maximum Age is 20 seconds.

**Note:** The above parameters (Hello Time, Maximum Age, and Forward Time) are constrained by the following formula:

$$(\text{Hello Time} + 1) \leq \text{Maximum Age} \leq 2 \times (\text{Forward Delay} - 1)$$

## Priority

Setting the bridge priority to a low value will increase the likelihood that the current bridge will become the root bridge. If the current bridge is located physically near the center of the network, decrease the Bridge Priority from its default value of 32768 to make it become the root bridge. If the current bridge is near the edge of the network, it is best to leave the value of the Bridge Priority at its default setting.

In general, reducing the values of these timers will make the spanning tree react faster when the topology changes, but may cause temporary loops as the tree stabilizes in its new configuration. Increasing the values of these timers will make the tree react more slowly to changes in topology, but will make an unintended reconfiguration less likely. All of the bridges on the network will use the values set by the root bridge. It is only necessary to reconfigure that bridge if changing the parameters.

## Port Priority

The port priority is a spanning tree parameter that ranks each port, so that if two or more ports have the same path cost, the STP selects the path with the highest priority (the lowest numerical value). By changing the priority of a port, it can be more, or less, likely to become the root port. The default value is 128, and the value range is 0–255.

## Port Path Cost

Port path cost is the spanning tree parameter that assigns a cost factor to each port. The lower the assigned port path cost is, the more likely that port will be accessed. The default port path cost for a 10 Mbps or 100 Mbps port is the result of the equation:

$$\text{Path cost} = 1000 / \text{LAN speed (in Mbps)}$$

Therefore, for 10 Mbps ports, the default port path cost is 100. For 100 Mbps ports, it is 10. To allow for faster networks, the port path cost for a 1000 Mbps port is set by the standard at 4.

## 5.5.2 Rapid Spanning Tree Protocol (RSTP)

Rapid Spanning Tree Protocol makes use of point-to-point link type and expedites into a rapid convergence of the spanning tree. Re-configuration of the spanning tree can occur in less than 1 second (as opposed to 50 seconds with the default settings in the legacy spanning tree), which is critical for networks carrying delay-sensitive traffic, such as voice and video.

### Port Roles and the Active Topology

RSTP provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. RSTP uses the same underlying spanning tree calculation and algorithm as legacy STP to select the bridge with the highest bridge priority (lowest numerical priority value) as the root bridge. Then RSTP assigns one of these port roles to bridge ports:

- Root port—provides the best path (lowest cost) when the bridge forwards packets to the root switch.

- Designated port—connects to the designated switch, which has the lowest path cost when forwarding packets from that LAN to the root bridge. The port through which the designated switch is attached to the LAN is called the designated port.
- Alternate port—offers an alternate path toward the root switch to that provided by the current root port.
- Backup port—acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected together in a loop-back by a point-to-point link or when a switch has two or more connections to a shared LAN segment.
- Disabled port—has no role in the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

### Rapid Convergence

RSTP provides for rapid recovery of connectivity following the failure of a switch, switch port, or LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- Edge ports—If a port on a switch running RSTP is assigned to be an edge port, it will be put to forwarding immediately. However, the edge port will be in the RSTP initialization state and will send out the RSTP BPDUs with the operating status of edge port set to TRUE. If the edge port starts receiving the BPDUs, it will change the operating edge state to FALSE and start the spanning tree calculations. It is recommended to assign any ports that are to be left as a “leaf” of the LAN (with no connection to any bridge) as edge ports.
- Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.
- Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

Note that if the link type of the port is not forced, the switch makes the decision of link type by operating duplex mode of the port. Also, a port with full-duplex mode is considered as a point-to-point link type, and a port in half-duplex mode is set as shared link type.

## 5.5.3 Configuring spanning-tree

### Enabling/Disabling Spanning-tree

Use the configuration mode command below to enable/disable spanning tree on the switch.

Command	Purpose
<b>spanning-tree forceversion 8021w</b>	Enable Rapid spanning-tree(802.1W) on the switch.
<b>spanning-tree forceversion none</b>	Disable spanning tree on the switch

### Configuring Switch/Bridge Priority

For <priority> the range is 0 to 61440 in increments of 4096; the default is 32768. The lower number is used when you want to specify the switch as the root switch.

Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Command	Purpose
<b>spanning-tree priority 8192</b>	Set switch priority to 8192

### Configuring Link Type

Use the following interface mode command to configure port link-type:

Command	Purpose
<b>spanning-tree port force-p2plink enable ports 1-2</b>	Set link type of port 1,2 to point to point

By default, the link type is determined from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection.

To return the switch to its default setting, use the **following** configuration command.

Command	Purpose
<b>spanning-tree port force-p2plink auto ports 1-2</b>	Set link type of port 1,2 to auto

### Configuring an Edge Port

Use the following interface mode command to configure port link type:

Command	Purpose
<b>spanning-tree port edge enable ports 1-2</b>	Set port 1,2 to edge port

The default setting is no edge port configuration.

To return the switch to its default setting, use the **following** configuration command.

Command	Purpose
<b>spanning-tree port edge disable ports 1-2</b>	Set port 1,2 to non edge port

### Configuring Port Path Cost

Use the following interface mode command to configure port path cost:

Command	Purpose
<b>spanning-tree port cost 1000 ports 1-2</b>	Set path cost of port 1,2 to 1000

The default values for path cost are determined by the operating port speed:

- For ports operating in 1000Mb speed, the path cost is 20000
- For ports operating in 100Mb speed, the path cost is 200000
- For ports operating in 10Mb speed, the path cost is 2000000

To return the switch to its default setting, use the **following** configuration command.

Command	Purpose
<b>spanning-tree port cost 0 ports 1-2</b>	Set path cost of ports 1,2 to default values

### Configuring Port Priority

Use the following interface mode command to configure port priority:

Command	Purpose
<b>spanning-tree port priority 10 ports 1-2</b>	Set priority of ports 1,2 to 10

For *<port-priority>*, the range is 0–240 in increments of 16; the default is 128. The lower the number, the higher the priority.

## Chapter 6: Configuring IP

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. All other IP protocols are built on the foundation. IP is a network-layer protocol that contains addressing and control information that allows data packets to be routed.

The table below lists the traditional classes and ranges of IP addresses and their status.

Class	Address or Range	Status
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.0.0.0 255.255.255.0	Available
C	192.0.0.0 to 223.255.255.0	Available
D	224.0.0.0 to 239.255.255.255	Multicast group addresses
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

With the rapid expansion of networks being connected to the Internet, critical problems were seen with the traditional classified addressing scheme. It was possible that IP addresses would run out, and routing tables would be overwhelmed. Thus, the Classless Inter-Domain Routing (CIDR) addressing scheme was created.

CIDR replaces the older process of assigning IP addresses with general prefixes of 8, 16, or 24 bits. CIDR uses prefixes of 13 to 27 bits. A CIDR address includes the standard 32-bit IP address and adds information on how many bits are used for the network prefix. In the IP address 206.203.1.35/27, the "/27" indicates that the first 27 bits are used to identify the unique network, and the remaining bits are used to identify the specific host. Now, blocks of addresses can be better fitted to even very small or very large networks.

The following table describes the Class C equivalent of CIDR prefixes.

CIDR Prefix	Class C Equivalent	Host Addresses
/27	1/8 Class C	32 Hosts
/26	1/4 Class C	64 Hosts
/25	1/2 Class C	128 Hosts
/24	1 Class C	256 Hosts
/23	2 Class C	512 Hosts
/22	4 Class C	1,024 Hosts
/21	8 Class C	2,048 Hosts
/20	16 Class C	4,096 Hosts

/19	32 Class C	8,192 Hosts
/18	64 Class C	16,384 Hosts
/17	128 Class C	32,768 Hosts
/16	256 Class C OR 1 Class B	65,536 Hosts
/13	2,048 Class C	524,288 Hosts

## 6.1 Establish Address Resolution

A device in the IP can have both a local address (which uniquely identifies the device on its local segment or LAN) and a network address (which identifies the network to which the device belongs). The local address is more properly known as a *data link* address because it is contained in the data link layer (Layer 2 of the OSI model) part of the packet header and is read by data link devices (bridges and all device interfaces, for example). The more technically inclined will refer to local addresses as *MAC addresses*, because the Media Access Control (MAC) sub-layer within the data link layer processes addresses for the layer.

To communicate with a device on Ethernet, you first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*. The IntraCore 3724PWR software uses the Address Resolution Protocol (ARP) for address resolution. ARP is used to associate IP addresses with media or MAC addresses. Taking an IP address as input, ARP determines the associated media address.

Once a media or MAC address is determined, the IP address/media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network.

## 6.2 Managing IP Multicast Traffic

Multicast traffic is a means to transmit a multimedia stream from the Internet (a video conference, for example) without requiring a TCP connection from every remote host that wants to receive the stream.

Traditional IP communication allows a host to send packets to one host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a group of hosts (group transmission). A multicast address is chosen for the members of a multicast group. Senders use that address as the destination address of a datagram to reach all hosts of the group. The stream is sent to the multicast address, and from there, it is delivered to all interested parties on the Internet. Any host, regardless of whether it is a member of a group, can send to that group. However, only the members of the group receive the message.

The IntraCore IC3724PWR supports the snooping of Internet Group Management Protocol (IGMP) messages that are used between hosts on a LAN and the switch(s)/routers on that LAN to track the multicast groups of which hosts are members. The switch supports IGMP Version 2 that has such features as the IGMP query timeout and the maximum query response time.

### 6.2.1 IGMP Overview

The Internet Group Management Protocol (IGMP) manages the multicast groups on a LAN. IP hosts use IGMP to report their group membership to directly connected multicast switches. Switches executing a multicast protocol maintain forwarding tables to forward multicast datagram's. Switches use the IGMP to learn whether members of a group are present on their directly attached sub-nets. Hosts join multicast groups by sending IGMP report messages.

IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

The address 224.0.0.0 will not be assigned to any group. The address 224.0.0.1 is assigned to all systems on a sub-net. The address 224.0.0.2 is assigned to all switches on a sub-net.

**Forwarding Unknown Multicast Packets. Unknown multicast packets are those packets with destination IP multicast addresses not learned by the switch. By default, the switch forwards all such traffic.**

### 6.2.2 Configuring IGMP

Use the following commands to configure IGMP.

#### **Enable the IGMP Snooping**

To enable/disable IGMP, use the command below. Unknown multicast traffic will not be forwarded once igmp is enabled.

Command	Purpose
Set igmp {enable   disable}	Enable/Disable IGMP



### Enable the IGMP querier

Multicast switches can send IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-systems group address of 224.0.0.1 with a time-to-live (TTL) value of 1.

Multicast switches continue to periodically send host-query messages to refresh their knowledge of memberships present on their networks. If, after some number of queries, the switch software discovers that no local hosts are members of a multicast group, the software stops forwarding onto the local network multicast packets from remote origins for that group and sends a prune message upstream toward the source.

The switch can be configured to send IGMP queries which are used to solicit IGMP hosts report messages. The switch uses the report messages to keep track of which ports belong to which IP multicast group.

To enable/disable IGMP querier , use the command below:

Command	Purpose
<b>set igmp-querier {enable   disable}</b>	Enable/Disable IGMP querier

### Modifying the IGMP Host-Query Message Interval

Multicast switches elect a designated switch for the LAN (subnet). The designated switch is the one with the highest IP address. The switch is responsible for sending IGMP host-query messages to all hosts on the LAN. By default, the designated switch sends IGMP host-query messages every 60 seconds in order to keep the IGMP overhead on hosts and networks very low. To modify this interval, use the following command in interface configuration mode:

Command	Purpose
<b>set igmp query-interval &lt;10-3600 seconds&gt;</b>	Configure the frequency at which the designated switch sends IGMP host-query messages.

The following example shows setting the IGMP query interval to 200.

```
Switch(config)# set igmp query-interval 200
```

### Changing the Maximum Query Response Time

By default, the maximum query response time advertised in IGMP queries is 10 seconds. If the switch is using IGMP Version 2, you can change this value. To change the maximum query response time, use the following command in configuration mode:

Command	Purpose
<b>set igmp query-resinterval &lt;0-200 seconds&gt;</b>	Set the maximum query response time advertised in IGMP queries.

## 6.3 Access Lists

An access list is a criteria statement that the switch uses to determine whether to allow or block traffic based on MAC addresses, IP addresses, or UDP/TCP ports. Access lists can be configured to provide basic security on your network, and to prevent unnecessary traffic between network segments. Access lists are applied to inbound traffic only.

When configuring an access list, an argument of 'priority' must be specified. The priority of an ACL is important, as the switch tests addresses of each packet against the criteria in access lists one by one (in the order of the priority) until it finds a match. One of the arguments in specifying the access list is the '**mask**' that comes after a MAC address or IP address. This argument identifies which bits in the address field are to be matched. A "1" indicates that positions must match; a "0" indicates that position is ignored

The check of a match comes first for an access list with lower priority(lower value) than those with higher priority values. The **last** match determines whether the software accepts or rejects the address. In case of multiple matches, the match in IP mode takes precedence over that in MAC mode. Because the switch goes through the whole set of access lists to find matches, the priority of the ACL is critical.

**Important!** By default, if no conditions match, the switch allows the address.

The switch supports up to 256 access lists, and MAC address based access lists can not exceed 64.

An access list can be configured using the command and its arguments in configuration mode below:

access-list name acl1 ?

add	Create a new access-list
action	Specify the action of the ACL entry
clear	Clear ACL entry contents
delete	Remove the ACL entry
enable	Enable the ACL entry
disable	Disable the ACL entry
set	Set ACL entry contents

### 6.3.1 Creating an Access List

To create an access list, use the command below:

Command	Purpose
access-list name acl1 add priority 1	Create an access list named 'acl_name' with priority 1

### 6.3.2 Configuring an Access List

To configure an access list, use the command below:

Command	Purpose
<b>access-list name acl1 set .....</b>	Set the criteria statement of an access list named 'acl_name'
<b>access-list name acl1 action .....</b>	Specify the action to take if criteria of the access list is matched

In the following example, an access list will be created to block traffic sent from MAC address 00-00-94-12-34-56.

```
Switch(Config)# access-list name acl_mac add priority 1

Switch(Config)# access-list name acl_mac set mac-mode macsa 00-00-94-12-34-56 ff-ff-ff-ff-ff-ff

Switch(Config)# access-list name acl_mac action deny

Switch(Config)#
```

In the next example, a standard access list will be created to deny all traffic from 192.168.123.254 , and allow all other traffic to be forwarded.

```
Switch(Config)# access-list name acl_ip add priority 1

Switch(Config)# access-list name acl_ip set ip-mode srcip 192.168.123.254 255.255.255.255

Switch(Config)# access-list name acl_ip action deny

Switch(Config)#
```

In the following example, an access list will be created to deny Telnet traffic.

```
Switch(Config)# access-list name acl_tcp_src add priority 1

Switch(Config)# access-list name acl_tcp_src set ip-mode l4port src-port from 23 to 23

Switch(Config)# access-list name acl_tcp_dst add priority 2

Switch(Config)# access-list name acl_tcp set ip-mode l4port dst-port from 23 to 23

Switch(Config)# access-list name acl_tcp_src action deny

Switch(Config)# access-list name acl_tcp_dst action deny

Switch(Config)#
```

### 6.3.3 Applying an Access List to an Interface

After creating your access lists, you can choose interfaces for which the access lists will be applied. If no interfaces are explicitly selected, the access list is applied to all interfaces.

To select the interface for an access list, use the following command:

Command	Purpose
<b>access-list name acl1 set portlist .....</b>	Select interfaces that the access list 'acl1' will be applied

In the next example, we will create an extended access list that will allow only SMTP bound traffic (port 25) to be forwarded on port 7, and deny all other traffic.

```
Switch(Config)# access-list name acl_tcp_dst_smtp add priority 1

Switch(Config)# access-list name acl_tcp_dst_smtp set ip-mode l4port dst-port from 25
to 25

Switch(Config)# access-list name acl_tcp_dst_smtp set portlist 7

Switch(Config)# access-list name acl_tcp_dst_smtp action permit

Switch(Config)# access-list name acl_deny_all add priority 2

Switch(Config)# access-list name acl_deny_all set ip-mode l4port dst-port from 25 to
25

Switch(Config)# access-list name acl_deny_all set mac-mode macsa 00-00-94-12-34-56 00-
00-00-00-00

Switch(Config)# access-list name acl_deny_all action deny
```

### 6.3.4 Enabling an Access List

To enable a configured access list, use the command below. All the examples above require execution of the 'enable' command to make the access lists effective.

Command	Purpose
<b>access-list name acl_name enable</b>	Enable an access list named 'acl_name'.

## Chapter 7: Power over Ethernet (PoE)

### 7.1 PoE Theory

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the need to place network devices next to a power source. Examples include:

- IP Phones
- Wireless Access Points
- IP Gateways
- Cameras
- Audio remote monitoring equipment

As technology has progressed, PoE has evolved. Equipment from many manufacturers, including the Asante IC3724PWR, supports the 802.3af standard. By default, the IC3724PWR is set to work with 802.3af compliant devices. The 802.3af standard includes the ability to determine when a compliant Powered Device (PD) is connected to a port. Power is only provided when a compliant device is detected. As per the standard, ports can be set to provide different amounts of power. The IC3724PWR also includes features that allow the switch to be configured differently to accommodate older, noncompliant equipment, using older detection methods, and to meet special needs.

**7.2 PoE Show Example** To access the PoE feature, login to the switch and enter the username and password. Next use the enable command to enter privileged mode. Once in enable mode, the show command can be used to view the switch PoE settings. An example appears below.

```
Login: admin
Password: *****
COMMAND> en
Username: admin
Password: *****
Switch# show
```

Using help (?) the PoE subcommands and their functions can be identified.

```
Switch#
```

```
Switch# show poe
```

```
system-status    Display PoE System Status
port-index       Specify an switch poe interface
all              Display all switch poe interface
```

```
Switch# show poe system-status
```

```
POE SW Version:    0.36
PoE   Number:      12
Total Allocation(0.1W): 1000
Guard Band(0.1W):   80
Management Mode:    Dynamic without priority
Total Consumption:  30700
```

```
Switch# show poe port-index
```

```
portindex(1,2,..) Switch poe interface index
```

```
Switch# show poe port-index 1
```

```
Port AdminStatus Priority P_allocation P_consumption P_detectiontype
```

---

```
1   Enable   NORMAL 15400    0      IEEE 802.3af 4-Point Detection only (Default)
```

```
Switch#
```

```
Switch# show poe all
```

```
Port AdminStatus Priority P_allocation P_consumption P_detectiontype
```

---

1	Enable	NORMAL	15400	8800	Legacy Capacitive Detection only
2	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
3	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
4	Enable	NORMAL	15400	2000	IEEE 802.3af 4-Point Detection only (Default)
5	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
6	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
13	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
14	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
15	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
16	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
17	Enable	NORMAL	15400	2900	IEEE 802.3af 4-Point Detection only (Default)
18	Enable	NORMAL	15400	2700	IEEE 802.3af 4-Point Detection only (Default)

```
Switch#
```

### 7.3 PoE Interface Mode

To change settings on a port, enter the configuration interface mode.

```
Switch(Interface 1)# poe
```

func	Configure poe function on a port
power-pri	Configure power priority on a port
detection	Configure detection type on a port
high-power	Configure Power Energy Mode on a port

**Func** is the setting that enables or disables the poe function on a particular port.

**Power-pri** selects the priority policy to determine which ports still receive power is the maximum is reached.

Static with priority: This mode considers the used power is port's allocation and PSE provides the power to the port with higher priority first.

Dynamic with priority: This mode considers the used power is port's consumption and PSE provides the power to the port with higher priority first.

Static without priority: This mode considers the used power is port's allocation and PSE first provides the power to the port which is first required.

Dynamic without priority: This mode considers the used power is port's consumption and PSE first provides the power to the port which is first required.

**Detection** Indicates which PoE detection type has been chosen.

No Detection: PSE will provide power to PD without detection.

Legacy Capacitive Detection only: PSE would provide three points to test PD's capacitance. After a PD is successfully detected, power is delivered to the port, or not.

IEEE 802.3af 4-Point Detection only (Default): PSE would provide four points voltage to test PD's resistance. After a PD is successfully detected, power is delivered to the port, or not.

IEEE 802.3af 4-Point followed by Legacy: PSE would provide four points voltage to test PD's capacitance. After a PD is successfully detected, power is delivered to the port, or not.

IEEE 802.3af 2-Point only: PSE would provide two points voltage to test PD's resistance. After a PD is successfully detected, power is delivered to the port, or not.

IEEE 802.3af 2-Point followed by Legacy: PSE would provide two points voltage to test PD's capacitance. After a PD is successfully detected, power is delivered to the port, or not.

**The first 2 options(No Detection, Legacy..) can be used for older legacy POE devices if the default detection method does not detect the PD.**

**High-power** enables or disables the 30 watt power limit mode. The default is 15 watts.

## 7.4 PoE Interface Settings Example

Here is an example of possible settings



Switch(Interface 1)# poe func

enable        Enable poe function on a port

disable       Disable poe function mode on a port

Switch(Interface 1)# poe power-pri

level        Power priority level

Switch(Interface 1)# poe power-pri level

low         Set to low priority

normal       Set to normal priority

middle       Set to middle priority

high         Set to high priority

Switch(Interface 1)# poe power-pri level normal

Switch(Interface 1)# poe detection

type        detection type

Switch(Interface 1)# poe detection type

0            No Detection

1            Legacy Capacitive Detection only

2            IEEE 802.3af 4-Point Detection only (Default)

3            IEEE 802.3af 4-Point followed by Legacy

4            IEEE 802.3af 2-Point only

5            IEEE 802.3af 2-Point followed by Legacy

Switch(Interface 1)# poe detection type 2

Switch(Interface 1)# poe high-power

status       detection type

Switch(Interface 1)# poe high-power status

on           start High Power Mode

off          End High Power Mode

Switch(Interface 1)# poe high-power status off

## Chapter 8: VLAN Configuration

VLANs are used to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group and eliminate broadcast storms in large networks. VLANs provide a secure and efficient network environment.

VLANs are based on untagged port groups, or traffic can be explicitly tagged to identify the VLAN group to which it belongs. Untagged VLANs can be used for small networks attached to a single switch. Tagged VLANs should be used for larger networks, and all the VLANs assigned to the inter-switch links.

Use the VLAN feature to partition a single IntraCore 3724PWR into a VLAN each containing its own set of ports. Packets are forwarded only between ports belonging to the same VLAN. This allows you to restrict access from one segment to another to increase network security or to reduce traffic. To set up VLANs you should specify the ports belonging to the VLAN, and setup of tagging. The following shows the commands available to configure VLAN's.

```
Switch(Config)# vlan ?
  add                Create a new VLAN
  delete            Remove a existed VLAN
  port              Configure 802.1Q port parameters for VLANs
  lag               Configure lag to a special VLAN
Switch(Config)# interface 4

Switch(Interface 4)# vlan ?

  participation      Join or leave a VLAN
  protected          Configure port protected property
  dropnq            Configure port drop no 8021q frame
  ingress           Configure port filter
  pvid              Configure port PVID
```

The switch is shipped with a default VLAN with VLAN ID (VID) 1. All switch ports are included in the default VID 1. **The default VID 1 cannot be deleted.**

Up to 256 Virtual LANs (VLANs) are supported on the IntraCore 3724PWR. The default VLAN with VLAN ID (VID) 1. All switch ports are included in the default VID 1. **The default VID 1 cannot be deleted.**

### 8.1 Creating or Modifying a VLAN

To create a VLAN with id 2, enter the following commands beginning in enabled mode:

```
Switch#
Switch# configuration
Switch(Config)# vlan
  add                Create a new VLAN
  delete            Remove a existed VLAN
  port              Configure 802.1Q port parameters for VLANs
  lag               Configure lag to a special VLAN
Switch(Config)# vlan add
```

```

number          Enter a VLAN ID
range          Enter a range of VLAN ID
Switch(Config)# vlan add number
<2..4094>      Enter a VLAN ID
Switch(Config)# vlan add number 2
Switch(Config)#

```

VLANS can be configured using the following commands:

<b>vlan add number 2</b>	Create vlan 2
<b>vlan add range from 3 to 6</b>	Create vlans 3,4,5,6
<b>vlan delete 3</b>	Delete vlan 3

## 8.2 VLAN Port Membership

Ports of VLANS can be configured by the commands below :

### 8.2.1 configuring vlan ports

Command	Purpose/Format
<b>vlan port {all   ports}.....</b>	This command is used to configure ports in a specific vlan. This configuration is applied to all ports or some of the ports specified by subsequent arguments

Use the following commands, beginning in configuration mode, to assign an IEEE 802.1q trunk port:

To create 3 vlans,2,3,4 with vlan 2 untagged port members 1,2,3,4, vlan 3 untagged port members 6,7,8,9, and vlan 4 untagged port members 11,12,13,14, enter the following commands beginning in configuration mode. Note that exclude is used so ports belong to various vlans exclusively:

Note that exclude is used in 3<sup>rd</sup> command so ports 3,5,7,8,9 belong exclusively to vlan 3:

```

Switch(Config)# vlan add number 2

Switch(Config)# vlan port ports port-configure 2 untagged 1-4

Switch(Config)# vlan port ports port-configure 1 exclude 1-4

Switch(Config)# vlan add number 3

Switch(Config)# vlan port ports port-configure 3 untagged 6-9

Switch(Config)# vlan port ports port-configure 1 exclude 6-9

```

```
Switch(Config)# vlan add number 4

Switch(Config)# vlan port ports port-configure 2 untagged 11-14

Switch(Config)# vlan port ports port-configure 1 exclude 11-14

Switch(Config)#
```

### 8.2.2 Trunk (IEEE 802.1q)

By default, a trunk port is a member of all VLANs.

Use the following commands, beginning in configuration mode, to assign an IEEE 802.1q trunk port:

Command	Purpose
<b>interface IFNUMBER</b>	Enter the interface number to access the interface configuration mode.
<b>Vlan participation</b>	This command designates the interface to be a member of a vlan  Use the <b>no</b> form of this command to reset to the default of static-access mode.

Continue with the example in previous section, the commands below are used to make port 20 an IEEE 802.1q trunk port:

```
Switch(Config)# interface 20

Switch(Interface 20)# vlan participation tagged 2

Switch(Interface 20)# vlan participation tagged 3

Switch(Interface 20)# vlan participation tagged 4
```

The trunk port accepts tagged and untagged frames. All the untagged frames are classified to the trunk port's native VLAN (the VLAN whose VID matches the port's PVID). The trunk port also sends out the frames as untagged for the native VLAN and tagged for other VLANs.

## Chapter 9: Quality of Service Configuration

Quality of Service (QoS) is a general term referring to various methods of traffic management you can employ on your network to ensure that traffic you identify as high-priority can use a sufficient share of the available bandwidth. The IC3724PWR internally has 4 COS queues per port with which a wide varieties of applications (Video/Audio) can be supported.

In QoS, packets are classified by the priority assigned to them. Packets can be assigned a priority in various ways. A packet can be assigned a priority based on the input port, 802.1P header or ACL. There are 8 priorities 0~7. Each packet is queued on one of the 4 internal queues based on its priority and queuing configuration. Queue 4 has the highest priority and queue 1 the lowest.

The IC3724PWR supports the following QoS methods:

- Weighted Round Robin
- 802.1P Priority Queuing
- IP precedence, DSCP and DSCP Remark
- Ingress Rate-Limit and Egress Traffic-Shaping

### 9.1 Scheduling algorithm

There are 2 methods to schedule a packet to be transmitted from the switch : strict priority, and weighed round robin.

In strict priority, the packet with the highest priority will be sent first, the lower priority packets will be sent only when all higher priority packets have been sent. Therefore a low priority packet will not be sent if higher priority packets are present all the time.

In weighed round robin, the higher priority will not be able to hog all the XMT resources. The resources are allocated based on the weight value associated with each queue. The service of a queue will stop when the resource is used up. Then the service will go to the next queue. This will proceed with the 4 queues in a round robin fashion.

#### 9.1.1 Configuring Weighted Round Robin

When Weighted Round Robin is enabled, the default settings are as follows:

Queue	Weight
1	1
2	2
3	4
4	8

One can change the weights assigned to each queue to alter the service priorities. Based on the default values, queue 4 will be allocated more resource, hence higher priority.

To set weighted round robin settings, use the following command in EXEC mode:

Command	Purpose
Switch<config>#qos scheduling [wrr   strict]	Set the scheduling method.
Switch<config>#qos wrr .....	Set the settings of the weighted round robin.

### 9.1.2 Monitoring Weighted Round Robin

To display information about weighted round robin settings, use the following command in EXEC mode:

Command	Purpose
show qos queue-settings	Displays the settings of the weighted round robin.

## 9.2 Priority Queuing

Priority Queuing (PQ) allows you to define how traffic is prioritized in the switch. There are 8 traffic priorities (0-7) and 4 internal queues. Each packet can be assigned a priority based on which port it comes in, 802.1P header, or IP precedence/DSCP in IP header if the packet is an IP packet. The QoS configurations determine how priority is assigned based on packet characteristics to cause the switch to place traffic into the four queues.

### 9.2.1 Priority Mapping

Each outgoing packets is assigned to one of the 4 internal queues. The assigned is based on the configuration of the mapping between priorities and queues. The default mapping is as follows:

Priorities	Queues
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4.

The default setting implies that priority 0 is the lowest and 7 the highest.

To change priority-queue mapping, use the following command in EXEC mode:

Command	Purpose
Switch<config>#qos cos .....	Set the mapping between 802.1P priorities and 4 internal queues

### 9.2.2 Port Based QOS

To set Port Based QOS, use the following command in EXEC mode:

Command	Purpose
Switch<config>#qos port-based ....	Set the priority of the port

### 9.2.3 802.1P Based QOS

A packet with an 802.1P header has a priority value which will be assigned to the packet by the switch.

### 9.2.4 IP Based QOS

The priority of an IP packet can be assigned based on the IP Precedence or DSCP value.

To set IP Precedence QOS, use the following command in EXEC mode:

Command	Purpose
Switch<config>#qos qos-advanced ip-precedence	Enable IP precedence QOS
Switch<config>#qos ip-precedence ...	Set mapping between IP precedence value and the internal queues.

To set DSCP QOS, use the following command in EXEC mode:

Command	Purpose
Switch<config>#qos qos-advanced dscp	Enable IP DSCP QOS
Switch<config>#qos dscp ...	Set mapping between DSCP value and the 8 priorities.



## 9.3 Traffic Shaping

Traffic shaping allows you to control the traffic going out from an interface in order to match its flow to the speed of the remote target interface. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

### 9.3.1 Configuring Traffic Shaping for an Interface

To configure traffic shaping for outbound traffic on an interface, use the following command in interface configuration mode:

Command	Purpose
<b>Switch&lt;config&gt;#interface 5</b>	Go to interface 5
<b>Switch&lt;interface 5&gt;#rate-limit egress ....</b>	Set the rate limit of interface 5

## 9.4 Rate Limiting

The rate-limit command allows you to control the amount of traffic coming in on a port.

To set rate limit on an interface 5, use the following command in EXEC mode:

Command	Purpose
<b>Switch&lt;config&gt;#interface 5</b>	Go to interface 5
<b>Switch&lt;interface 5&gt;#rate-limit ingress ....</b>	Set the rate limit of interface 5

## Chapter 10: Configuring the Switch Using the GUI

This chapter provides an overview of configuring the switch with the graphical user interface (GUI). For more information about the different features and how to implement them refer to the chapters specific to that function.

At your web browser enter the IP address for the switch to launch the GUI. Depending on settings, you may receive a certificate error message. Ignore this and continue.

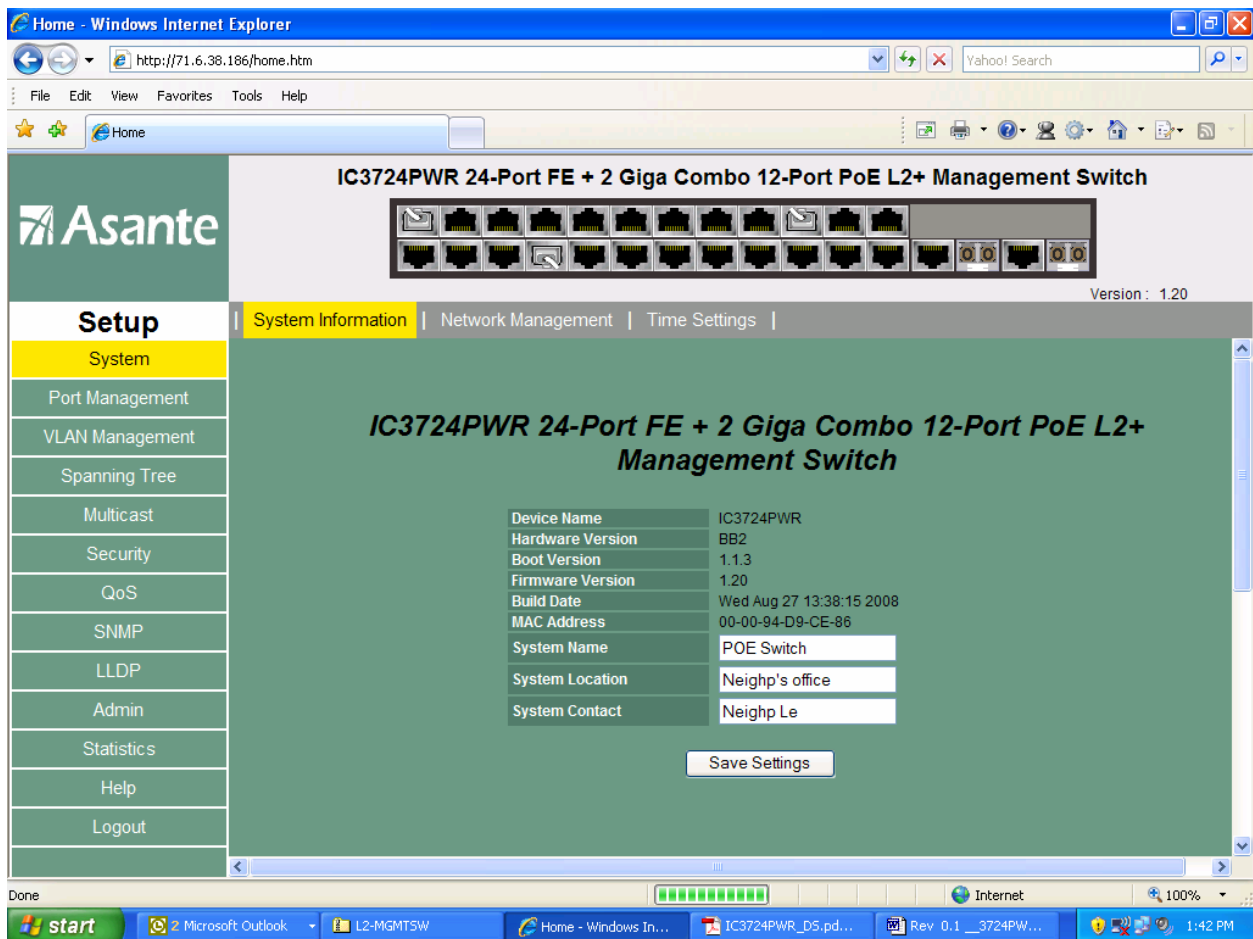
The defaults are:

IP Address: 192.168.0.1

Username: admin

Password: Asante (capital A)

Enter the username and password then click the “OK” button.



## 10.1 Main Configuration Menu

Use the navigation panel on the left side of the GUI screen to configure the switch. From this panel you can access the following screens:

- System
- Port Management (including PoE)
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin
- Statistics
- Help
- Logout

The following example shows the main Configuration Menu.



## 10.2 System

Use this section to access general information about the switch.

### 10.2.1 System Information

With the first system screen up a name and location for the switch can be added. A system contact can also be entered. You can also view the Hardware Version, Boot Version, Firmware Version, Build Date and the MAC Address. Save the settings when done by clicking the “Save Settings” button.

**Asante** IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch

Version: 1.20

Setup | System Information | Network Management | Time Settings

System

- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin
- Statistics
- Help
- Logout

**IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch**

Device Name	IC3724PWR
Hardware Version	BB2
Boot Version	1.1.3
Firmware Version	1.20
Build Date	Wed Aug 27 13:38:15 2008
MAC Address	00-00-94-D9-CE-86
System Name	<input type="text" value="POE Switch"/>
System Location	<input type="text" value="Neighp's office"/>
System Contact	<input type="text" value="Neighp Le"/>

## 10.2.2 System Network management.

This page allows the setting of static IP information. The switch can also be set to receive an address automatically from a DHCP server. The switch ships with the default IP address **192.168.0.1**.

Click the “Save Settings” button when done.

The screenshot displays the Asante web management interface for an IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch. The interface includes a navigation menu on the left with options like System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, LLDP, Admin, Statistics, Help, and Logout. The main content area shows the Network Management configuration page with the following settings:

IP Address Mode	Static
IP Address	71.6.38.186
Subnet Mask	255.255.255.192
Default Gateway	71.6.38.129
Management VLAN	1

A "Save Settings" button is located below the configuration fields. The interface also shows a "G2" logo and "Version: 1.2" in the top right corner.

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. All other IP protocols are built on the foundation. IP is a network-layer protocol that contains addressing and control information that allows data packets to be routed.

This section describes how to configure the Internet Protocol (IP). A number of tasks are associated with configuring IP. A basic and required task for configuring IP is to assign IP addresses to network interfaces. Doing so enables the interfaces and allows communication with hosts on those interfaces using IP. Associated with this task are decisions about subnetting and masking the IP addresses.

An IP address is a location to and from which IP datagrams can be sent. IP addresses were traditionally divided into three classes. The Class A Internet address format allocated the highest eight bits to the network field and set the highest-order bit to 0 (zero). The remaining 24 bits formed the host field. The Class B Internet address allocated the highest 16 bits to the network field and set the two highest-order bits to 1, 0. The remaining 16 bits formed the host field. The Class C Internet address allocated the highest 24 bits to the network field and set the three highest-order bits to 1,1,0. The remaining eight bits formed the host field.

The table below lists the traditional classes and ranges of IP addresses and their status.

<b>Class</b>	<b>Address or Range</b>	<b>Status</b>
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.0.0.0 255.255.255.0	Available
C	192.0.0.0 to 223.255.255.0	Available
D	224.0.0.0 to 239.255.255.255	Multicast group addresses
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

When multiple networks are connected to the Internet the traditional classified addressing scheme could cause you to run out of IP addresses.

The usual way of assigning IP addresses uses the prefixes of 8, 16, or 24 bits. Using prefixes of 13 to 27 bits an address includes the standard 32-bit IP address and adds information on how many bits are used for the network prefix. In the IP address 206.203.1.35/27, the "/27" indicates that the first 27 bits are used to identify the unique network, and the remaining bits are used to identify the specific host.

## 10.2.3 System Time Setting

Use the Time Setting page to set the time zone or local time for the switch. Daylight savings can also be enabled. Click the “Save Settings” button when done.

The screenshot shows the web interface for an Asante IC3724PWR switch. The page title is "IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch". The Asante logo is in the top left. A navigation menu on the left includes "Setup" (highlighted), "System Information", "Network Management", and "Time Settings" (highlighted). The "Time Settings" page has a sidebar with options: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, LLDP, Admin, Statistics, and Help. The main content area shows the following settings:

- Enable Daylight Saving
- Time Zone: (GMT-08:00) Pacific Time (US & Canada): Tijuana
- Use SNTP Server
  - Server IP Address: 207.46.232.182
  - Update Time Now button
  - Polling Interval: 12 hours
- Use Local Time
  - Time fields: M (9), D (12), Y (2008), H (12), M (58), S (42)
  - Use Browser Time button
- Save Settings button

### 10.3 Port Management – Port Config

The Port Management section displays assorted settings for each port.

**IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch**

Version: 1.20

**Setup** | **Port Config** | LACP Property | LAG Group | PoE |

Port	Link Status	Auto-Nego	Speed & Duplex	Flow Control
01	Up	Enable	100Mbps Full	Disabled
02	Down	Enable	--	--
03	Down	Enable	--	--
04	Down	Enable	--	--
05	Down	Enable	--	--
06	Down	Enable	--	--
07	Down	Enable	--	--
08	Down	Enable	--	--
09	Down	Enable	--	--
10	Up	Enable	100Mbps Full	Disabled
11	Down	Enable	--	--
12	Down	Enable	--	--
13	Down	Enable	--	--
14	Down	Enable	--	--
15	Down	Enable	--	--
16	Up	Enable	100Mbps Full	Disabled
17	Down	Enable	--	--
18	Down	Enable	--	--
19	Down	Enable	--	--
20	Down	Enable	--	--
21	Down	Enable	--	--
22	Down	Enable	--	--
23	Down	Enable	--	--
24	Down	Enable	--	--
G1	Down	Enable	--	--
G2	Down	Enable	--	--

Waiting for http://71.6.38.186/hidden.htm... Internet 100%



**Port Management – Port Config - Specific Port.** Settings can be made on a per port basis. When a port number is clicked the subscreen appears.

The screenshot shows a web-based configuration interface. On the left is a vertical sidebar menu under the heading "Setup". The menu items are: System, Port Management (highlighted in yellow), VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, and LLDP. The main content area has a breadcrumb trail: "Port Config | LACP Property | LAG Group". Below the breadcrumb is a table with the following data:

Port Number	Admin Mode	Auto Negotiation	Speed Duplex	Flow Control	LAG Group
02	Enable	Enable	10M Half	Disable	--

Below the table is a "Save Settings" button.

**Port management – LACP Property.** The LACP properties are displayed on this screen. The system LACP Priority can be set here. By clicking on a port number, a subscreen for each port is available.

**IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch**

Version: 1.20

Setup | Port Config | **LACP Property** | LAG Group | PoE |

LACP System Priority:  (0 - 65535)

Port Number	Priority	Admin Key	LAG Group	Status
<a href="#">01</a>	1001	1000	N/A	
<a href="#">02</a>	1002	1000	N/A	
<a href="#">03</a>	1003	1000	N/A	
<a href="#">04</a>	1004	1000	N/A	
<a href="#">05</a>	1005	1000	N/A	
<a href="#">06</a>	1006	1000	N/A	
<a href="#">07</a>	1007	1000	N/A	
<a href="#">08</a>	1008	1000	N/A	
<a href="#">09</a>	1009	1000	N/A	
<a href="#">10</a>	1010	1000	N/A	
<a href="#">11</a>	1011	1000	N/A	
<a href="#">12</a>	1012	1000	N/A	
<a href="#">13</a>	1013	1000	N/A	
<a href="#">14</a>	1014	1000	N/A	
<a href="#">15</a>	1015	1000	N/A	
<a href="#">16</a>	1016	1000	N/A	
<a href="#">17</a>	1017	1000	N/A	
<a href="#">18</a>	1018	1000	N/A	
<a href="#">19</a>	1019	1000	N/A	
<a href="#">20</a>	1020	1000	N/A	
<a href="#">21</a>	1021	1000	N/A	
<a href="#">22</a>	1022	1000	N/A	
<a href="#">23</a>	1023	1000	N/A	
<a href="#">24</a>	1024	1000	N/A	
<a href="#">G1</a>	1025	1000	N/A	
<a href="#">G2</a>	1026	1000	N/A	

**Port Management – LACP Property – Port.** Settings for each port can be entered.

The screenshot shows the 'LACP Properties for Port 02' configuration page. The left sidebar contains a 'Setup' menu with options: System, Port Management (highlighted), VLAN Management, Spanning Tree, Multicast, Security, and QoS. The main content area has a breadcrumb trail: Port Config | LACP Property | LAG Group. Below the title, there are two input fields: 'Admin Key' with the value '1000' and 'LACP Port Priority' with the value '1002'. A 'Save Settings' button is located below these fields.

**Port Management – LAG Group.** Click on a group number to set the groups properties.

The screenshot displays the 'LAG Group' configuration page for the 'IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch'. The left sidebar shows the 'Setup' menu with 'Port Management' selected. The main content area features a breadcrumb trail: Port Config | LACP Property | LAG Group | PoE. Above the table is a diagram of the switch's ports. The table below lists the LAG groups and their properties:

LAG Group	Port Member	Link Status	Speed Duplex
01	N/A	Down	--
02	N/A	Down	--
03	N/A	Down	--
04	N/A	Down	--
05	N/A	Down	--
06	N/A	Down	--

**Port Management – LAG Group - Each Group.** Once a link aggregation group is specified, the screen below can be used to add ports to the group.

**Asante** IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch

Version : 1.2

Setup | Port Config | LACP Property | **LAG Group** | PoE

System

**Port Management**

VLAN Management

Spanning Tree

Multicast

Security

QoS

SNMP

LLDP

LAG LAG01

01	02	03	04	05	06	07	08	09	10	11	12
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G1	G2										
<input type="checkbox"/>	<input type="checkbox"/>										

Save Settings

## 10.3.1 PoE

### Configuring POE

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources. The PoE Settings Page contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps. The PoE Settings Page displays the currently configured PoE ports and contains the following information:

**System Power Management Mode:** The possible values are,

Static with priority: This mode considers the used power is port's allocation and PSE provides the power to the port with higher priority first.

Dynamic with priority: This mode considers the used power is port's consumption and PSE provides the power to the port with higher priority first.

Static without priority: This mode considers the used power is port's allocation and PSE first provides the power to the port which is first required.

Dynamic without priority: This mode considers the used power is port's consumption and PSE first provides the power to the port which is first required.

**Power Total Allocation:** The maximum power which PSE will allow to supply .

**Guard Band:** The reserved power which PSE reserves for security.

**Total Power Consumption:** The power which the all PDs consume.

**Port:** specific port number. Click it to show and configure POE properties for this port.

**Admin Status:** Indicates whether PoE is enabled or disabled on the port.

**Power Priority:** Indicates this port's poe priority. The possible values are High, > Middle, > Normal, > Low. The default value is Normal.

**Power Allocation (milliwatts):** Indicates this port's allocation. The default value is 15.4W.

**Power Consumption (milliwatts):** Indicates the power value which this port's PD uses up.

**Detection Type:** Indicates which PoE detection type has been chosen.



**Setup**

Port Config | LACP Property | LAG Group | **PoE**

- System
- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin
- Statistics
- Help
- Logout

System Power Management Mode: Dynamic with priority

Power Total Allocation: 100000mW

Guard Band: 8000mW

Total Power Consumption: 11600mW

Port Number	Admin Status	Power Priority	Power Allocation(milliwatts)	Power Consumption (milliwatts)	Detection Type
01	Enabled	Normal	15400	9600	Legacy Capacitive Detection only
02	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
03	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
04	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
05	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
06	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
13	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
14	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
15	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
16	Enabled	Normal	15400	2000	IEEE 802.3af 4-Point Detection only (Default)
17	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)
18	Enabled	Normal	15400	0	IEEE 802.3af 4-Point Detection only (Default)



**Setup**

Port Config | LACP Property | LAG Group | **PoE**

- System
- Port Management**
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin
- Statistics
- Help
- Logout

**Config POE Properties for Port 01**

Enable PoE :	<input checked="" type="checkbox"/>
High Power Mode :	Off
Power Priority Level :	Normal
PoE Detection Type :	Legacy Capacitive Detection only
<div style="border: 1px solid black; padding: 2px;">Save Settings</div>	

- No Detection
- Legacy Capacitive Detection only
- IEEE 802.3af 4-Point Detection only (Default)
- IEEE 802.3af 4-Point followed by Legacy
- IEEE 802.3af 2-Point only
- IEEE 802.3af 2-Point followed by Legacy

**10.4 VLAN Management.** VLANs are used to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group and eliminate broadcast storms in large networks. VLANs provide a secure and efficient network environment.

VLANs are based on untagged port groups, or traffic can be explicitly tagged to identify the VLAN group to which it belongs. Untagged VLANs can be used for small networks attached to a single switch. Tagged VLANs should be used for larger networks, and all the VLANs assigned to the inter-switch links.

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs is assigned. LAN port VLAN membership is assigned manually on a port-by-port basis. VLANs can be defined as either Layer 2 or Layer 3 and a VLAN cannot switch between the two layers. Before you create a VLAN, you must decide how they will be created and a naming convention to ensure duplicate VLAN names are not used.

Up to 4094 Virtual LANs (VLANs) are supported on the IntraCore IC3724PWR. The default VLAN with VLAN ID (VID) 1. All switchports (eth1–eth24) are included in the default VID 1. **The default VID 1 cannot be deleted.**



Use this screen to view VLAN information and create a VLAN group. At the top of the main VLAN screen you can toggle between VLAN group information and VLAN port information by click on each link.

VLANs can be created one at a time, or a range of VLANS can be created all at once.

**IC3724PWR 24-Port FE + 2 Giga Combo 12-Port PoE L2+ Management Switch**

Version : 1.20

**Setup**

- System
- Port Management
- VLAN Management**
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin
- Statistics
- Help
- Logout

**Create VLAN** | VLAN Settings | VLAN Port

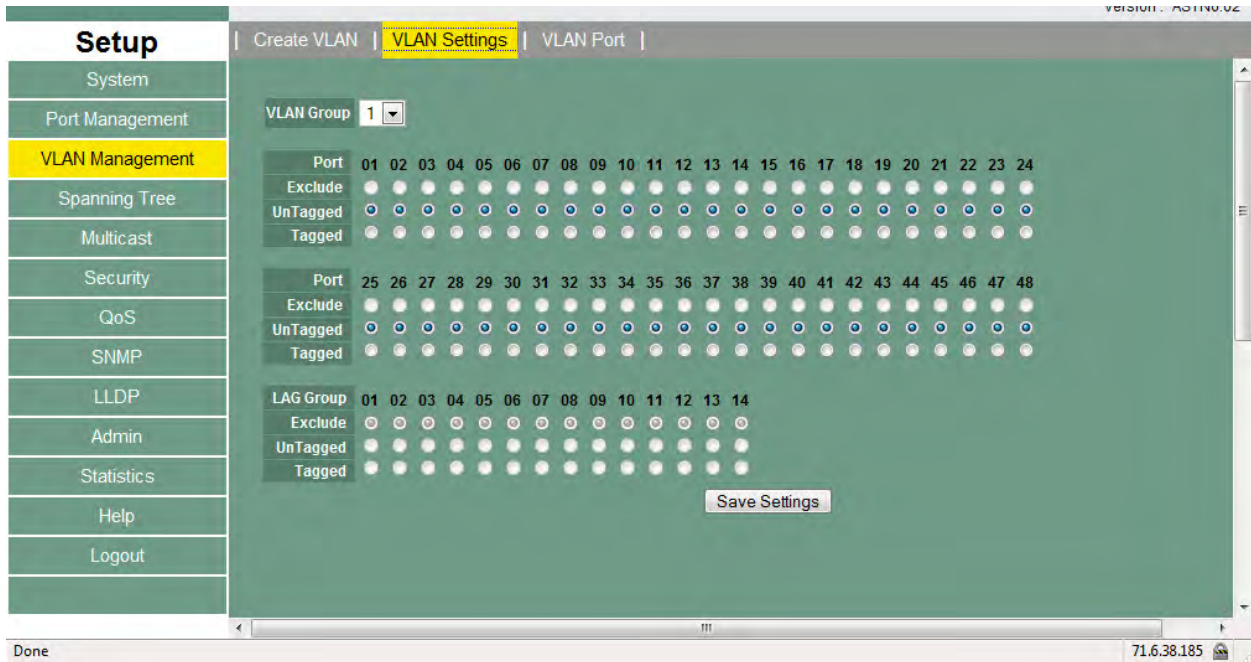
Single VLAN   (VLAN ID: 2-4094)

Multiple VLAN  -   (Low - High)

VLAN Ingress Filter :  Forward  Drop  Bypass

VLAN ID	Member ports	Tagged	Untagged	Delete
1	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 G1 G2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Delete
100	17 18 19 20 21 22 23 24	<input type="checkbox"/>	<input type="checkbox"/>	Delete

**VLAN MANAGEMENT – VLAN SETTINGS.** With a vlan selected, ports can be marked as tagged, or untagged. Lower on the screen, LAG groups can also be tagged or untagged. Click Save Settings when done.



**VLAN MANAGEMENT – VLAN PORT.** This screen allows additional settings to be controlled on a per port basis. Here the PVID can be changed to. Changing the PVID is required to force the port to respond to a particular VLAN. Becoming a member of a VLAN is only the start. The port PVID must be changed to cause it to respond only to the desired VLAN.

Various filters can be set on this screen. Ingress filter, Non 802.1Q filter, and port protection can all be set here.

Version: ASTN0.02

**Setup** | Create VLAN | VLAN Settings | **VLAN Port**

Port Number	PVID	Protected Port	Drop Non1Q Frame	VLAN Ingress Filter
01	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
02	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
03	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
04	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
05	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
06	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
08	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
09	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 10.5 Spanning Tree.

RSTP (Rapid spanning tree protocol) can be enabled at this screen. Various timer settings can also be set. Use this screen to change the priority and the path cost for specific ports. The priority default value is 128, and the value range is 0–240 (in multiples of 16).

The lower the assigned port path cost is, the more likely that port will be accessed. The default port path cost for a 10 Mbps or 100 Mbps port is the result of the equation:

$$\text{Path cost} = 1000/\text{LAN speed (in Mbps)}$$

Therefore, for 10 Mbps ports, the default port path cost is 100. For 100 Mbps ports, it is 10. To allow for faster networks, the port path cost for a 1000 Mbps port is set by the standard at 4.

The default values for path cost is determined by the operating port speed:

- For ports operating in 1000Mb speed, the path cost is 20000
- For ports operating in 100Mb speed, the path cost is 200000

For ports operating in 10Mb speed, the path cost is 2000000

The screenshot shows the configuration page for Spanning Tree. The left sidebar has a menu with 'Spanning Tree' highlighted. The main content area has a breadcrumb trail: 'Setup' > 'RSTP' > 'RSTP Port' > 'MSTP' > 'MSTP Port' > 'MSTP Instance' > 'MSTP Interface'. Below the breadcrumb, there is a checkbox labeled 'Enable RSTP' which is checked. A table displays the following settings:

Property	Bridge Setting	Root Status
Priority (0 - 61440)	32768	32768
Max Age (6-40 sec)	20	20
Forward Delay (4-30 sec)	15	15
Designated Root Bridge		_____

Below the table is a 'Save Settings' button.

RSTP can be designated on a port by port basis.

Use this screen to change the priority and the path cost for specific ports. The priority default value is 128, and the value range is 0–240 (in multiples of 16).

The lower the assigned port path cost is, the more likely that port will be accessed. The default port path cost for a 10 Mbps or 100 Mbps port is the result of the equation:

$$\text{Path cost} = 1000/\text{LAN speed (in Mbps)}$$

Therefore, for 10 Mbps ports, the default port path cost is 100. For 100 Mbps ports, it is 10. To allow for faster networks, the port path cost for a 1000 Mbps port is set by the standard at 4.

The default values for path cost is determined by the operating port speed:

- For ports operating in 1000Mb speed, the path cost is 20000
- For ports operating in 100Mb speed, the path cost is 200000

For ports operating in 10Mb speed, the path cost is 2000000

Setup		RSTP	RSTP Port	MSTP	MSTP Port	MSTP Instance	MSTP Interface	
System								
Port Management								
VLAN Management								
Spanning Tree								
Multicast								
Security								
QoS								
SNMP								
LLDP								
Admin								
Statistics								
Help								
Logout								
	Port	Participate	Cost	Priority	Edge	P2P	Status	Role
	01	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	02	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	03	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	04	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	05	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	06	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	07	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	08	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	09	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	10	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	11	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	12	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	13	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	14	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-
	15	<input checked="" type="checkbox"/> Yes	-	-	-	-	-	-

**MSTP.** Multiple Spanning Tree Protocol can be enabled on this page.

Individual Port properties can be manipulated at this screen.

The screenshot shows a web-based configuration interface for MSTP. On the left is a vertical navigation menu with the following items: Setup, System, Port Management, VLAN Management, Spanning Tree (highlighted in yellow), Multicast, Security, QoS, SNMP, LLDP, Admin, Statistics, Help, and Logout. The main content area is titled 'MSTP Port Settings' and includes a breadcrumb trail: RSTP | RSTP Port | MSTP | **MSTP Port** | MSTP Instance | MSTP Interface. A link for 'MSTP Port Priority & Path Cost Settings' is visible in the top right. The central part of the page contains a table with the following data:

Port	Edge	P2P	Migration Check
01	-	-	-
02	-	-	-
03	-	-	-
04	-	-	-
05	-	-	-
06	-	-	-
07	-	-	-
08	-	-	-
09	-	-	-
10	-	-	-
11	-	-	-
12	-	-	-
13	-	-	-
14	-	-	-
15	-	-	-
16	-	-	-
17	-	-	-
18	-	-	-
19	-	-	-
20	-	-	-

At the bottom of the interface, there is a status bar with the text 'Done' on the left and the IP address '71.6.38.185' on the right.



MST Instance parameters can be modified on the following two screens.

**Setup** | RSTP | RSTP Port | MSTP | MSTP Port | **MSTP Instance** | MSTP Interface

MST Instance: 0  
MST ID (0-4094):  
VLAN Range:

Add Remove Remove Last MST Instance

MST Instance	MST ID	VLAN Members
0	0	

Instance	Bridge Priority
0	-

Change Bridge Priority

**Setup** | RSTP | RSTP Port | MSTP | MSTP Port | MSTP Instance | **MSTP Interface**

Instance: 0

Port	Path Cost	Priority	Edge	P2P	Port Status	Port Role
01	-	-	-	-	-	-
02	-	-	-	-	-	-
03	-	-	-	-	-	-
04	-	-	-	-	-	-
05	-	-	-	-	-	-
06	-	-	-	-	-	-
07	-	-	-	-	-	-
08	-	-	-	-	-	-
09	-	-	-	-	-	-
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-
14	-	-	-	-	-	-
15	-	-	-	-	-	-
16	-	-	-	-	-	-
17	-	-	-	-	-	-
18	-	-	-	-	-	-
19	-	-	-	-	-	-
20	-	-	-	-	-	-
21	-	-	-	-	-	-
22	-	-	-	-	-	-

Done 71.6.38.185

## 10.6 Multicast.

Static multicast settings can be set. Port by port participation can be controlled.

The screenshot shows the 'Static Multicast' configuration page. On the left is a 'Setup' menu with options: System, Port Management, VLAN Management, Spanning Tree, **Multicast**, Security, QoS, SNMP, LLDP, Admin, Statistics, Help, and Logout. The main area has a breadcrumb trail: 'Static Multicast | Static Multicast Table | IGMP'. It contains three input fields: 'Group Name' (Max. 8 characters), 'VLAN ID' (1 ~ 4094), and 'MAC Address' (01:xx:xx:xx:xx:xx). Below these is a grid of checkboxes for ports 01 through 48. A 'Create..' button is centered at the bottom. The status bar at the bottom shows 'Done' on the left and '71.6.38.185' on the right.

The screenshot shows the 'Static Multicast Table' configuration page. The breadcrumb trail is 'Static Multicast | **Static Multicast Table** | IGMP'. A message at the top right states 'The Maximum Number of Multicast Groups is 128'. Below this is a table with the following columns: Group ID, Group Name, VLAN ID, Multicast Address, Member Port, Modify, and Delete. A 'Save Settings' button is centered below the table. The left 'Setup' menu is identical to the previous screenshot.

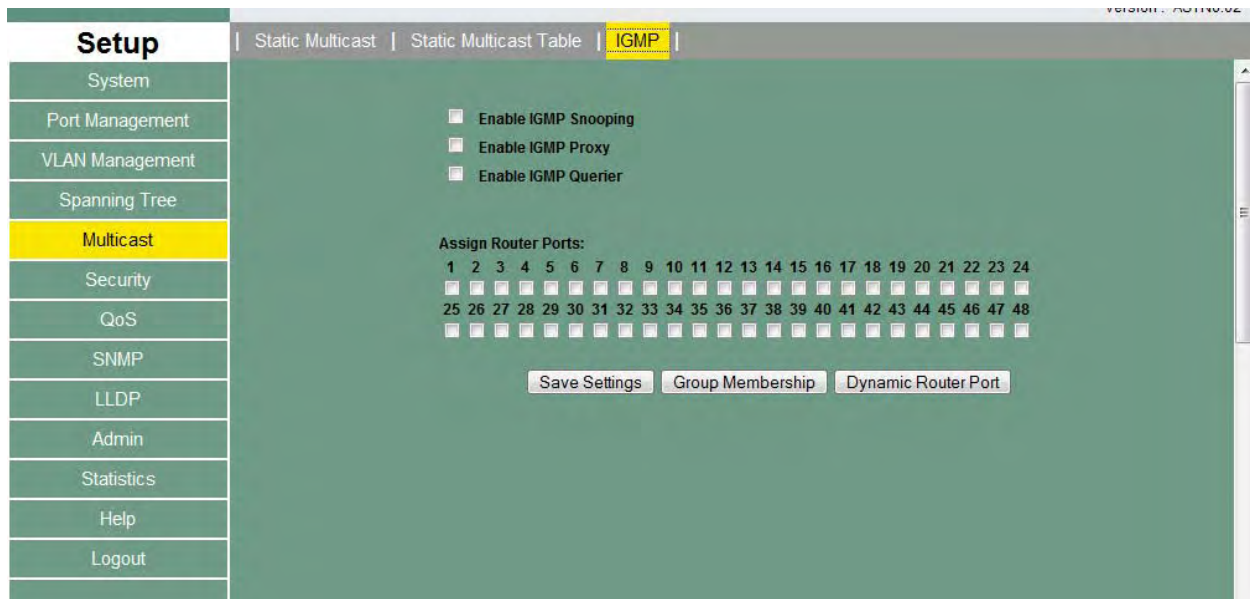


**IGMP** The Internet Group Management Protocol (IGMP) manages the multicast groups on a LAN. IP hosts use IGMP to report their group membership to directly connected multicast switches. Switches executing a multicast routing protocol maintain forwarding tables to forward multicast datagrams. Switches use the IGMP to learn whether members of a group are present on their directly attached sub-nets. Hosts join multicast groups by sending IGMP report messages.

IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

The address 224.0.0.0 will not be assigned to any group. The address 224.0.0.1 is assigned to all systems on a sub-net. The address 224.0.0.2 is assigned to all switches on a sub-net.

Multicast switches elect a designated switch for the LAN (subnet). The designated switch is the one with the highest IP address. The switch is responsible for sending IGMP host-query messages to all hosts on the LAN. By default, the designated switch sends IGMP host-query messages every 60 seconds in order to keep the IGMP overhead on hosts and networks very low. IGMP snooping allows multicasts to be pruned to only the ports whose users have requested the multicast. IGMP Querier should be enabled on one device on you local network. That querier actively determines which ports of which devices request multicast service.



Multicast switches send IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-systems group address of 224.0.0.1 with a time-to-live (TTL) value of 1.

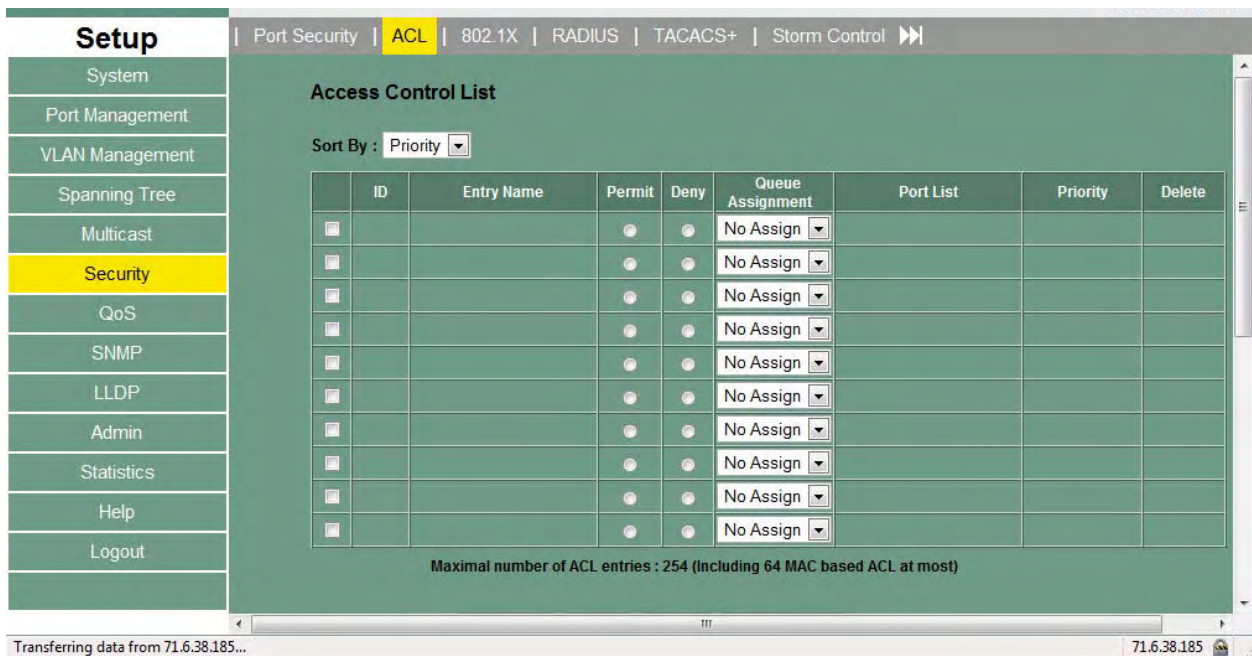
Multicast switches continue to periodically send host-query messages to refresh their knowledge of memberships present on their networks. If, after some number of queries, the switch software discovers that no local hosts are members of a multicast group, the software stops forwarding onto the local network multicast packets from remote origins for that group and sends a prune message upstream toward the source.

## 10.7 Security - Port Security.

Each port can be listed individually or a table can be displayed using the Show Table button



Access control lists can be established using this screen.



802.1X can be enabled on a per port basis

Setup | Port Security | ACL | 802.1X | RADIUS | TACACS+ | Storm Control

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
**Security**  
QoS  
SNMP  
LLDP  
Admin  
Statistics  
Help  
Logout

Enable 802.1X

Port	Status	Client MAC Address	Authorization
01	<input checked="" type="checkbox"/> Enabled		N/A
02	<input checked="" type="checkbox"/> Enabled		N/A
03	<input checked="" type="checkbox"/> Enabled		N/A
04	<input checked="" type="checkbox"/> Enabled		N/A
05	<input checked="" type="checkbox"/> Enabled		N/A
06	<input checked="" type="checkbox"/> Enabled		N/A
07	<input checked="" type="checkbox"/> Enabled		N/A
08	<input checked="" type="checkbox"/> Enabled		N/A
09	<input checked="" type="checkbox"/> Enabled		N/A
10	<input checked="" type="checkbox"/> Enabled		N/A
11	<input checked="" type="checkbox"/> Enabled		N/A
12	<input checked="" type="checkbox"/> Enabled		N/A
13	<input checked="" type="checkbox"/> Enabled		N/A

https://71.6.38.185/dot1x.htm 71.6.38.185

Radius server can be identified at this screen. A secret key can be created and the port can be altered.

Setup | Port Security | ACL | 802.1X | RADIUS | TACACS+ | Storm Control

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
**Security**  
QoS  
SNMP  
LLDP  
Admin  
Statistics  
Help  
Logout

RADIUS Server IP Address 0 0 0 0  
Authorization Port 1812  
Secret Key String

Save Settings

**TACAS+** and **Storm Control** are available on the next screens.

Version: ASTN0.02

Port Security | ACL | 802.1X | RADIUS | **TACACS+** | Storm Control

Authentication Type: TACACS+ And Local

TACACS+ Server: [ADD](#)

ID	Server IP Address	Priority	Authentication Port	Timeout for Retry	Delete
0	192.108.250.76	0	49	10	<a href="#">DELETE</a>

Maximal number of Servers : 2

Save Settings

Setup menu items: System, Port Management, VLAN Management, Spanning Tree, Multicast, **Security**, QoS, SNMP, LLDP, Admin, Statistics, Help, Logout

Port Security | ACL | 802.1X | RADIUS | TACACS+ | **Storm Control**

Port: All

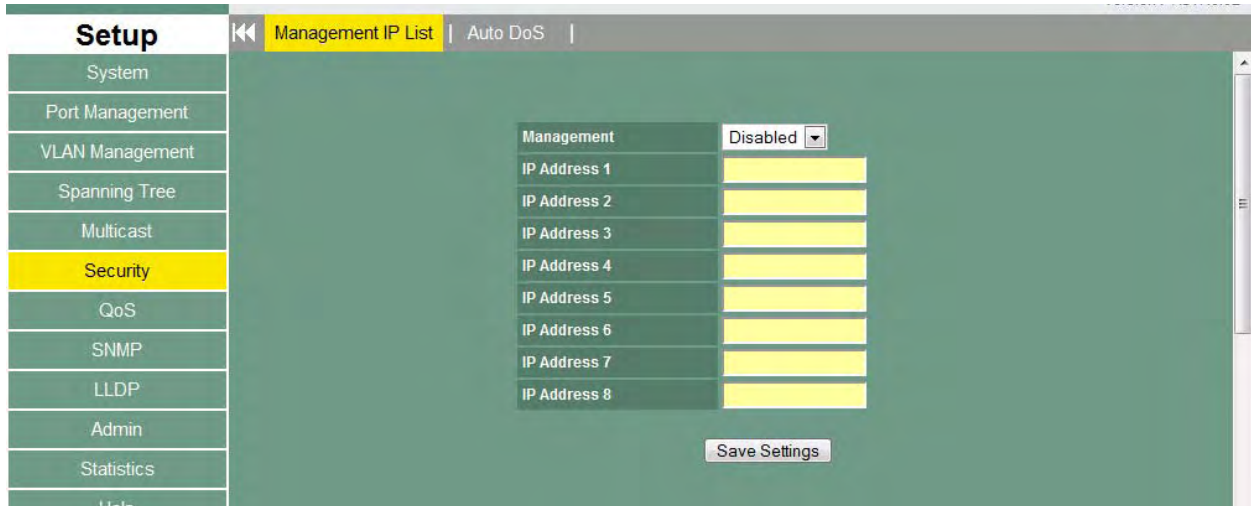
Control Type: None

Control Rate: 10 pps

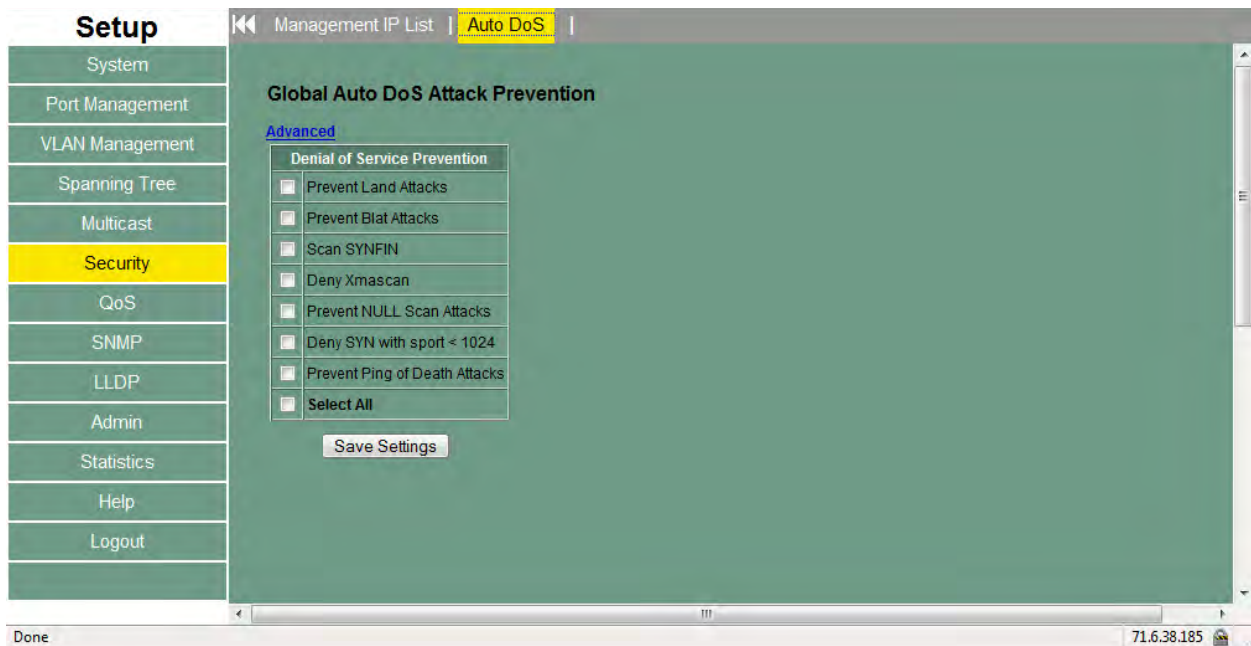
Save Settings Show Control Table

Setup menu items: System, Port Management, VLAN Management, Spanning Tree, Multicast, **Security**, QoS, SNMP, LLDP, Admin, Statistics

**Management IP list** can be used to enter a list of IP addresses to limit the availability of switch Management.



**Auto DoS** provides protection from a variety of denial of service type of threats.





## 10.8 QoS.

Quality of service settings allow various protocols to be selected to protect functions that require real time performance and limit other traffic.

The screenshot shows a web-based configuration interface for Quality of Service (QoS). On the left is a vertical navigation menu with the following items: Setup, System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS (highlighted in yellow), SNMP, LLDP, Admin, Statistics, Help, and Logout. The main content area is titled "Queue Settings" and includes a breadcrumb trail: Queue Settings | DSCP | 802.1P | Port-based QoS | Rate Control | DSCP Remark. The "Scheduling Mode" is set to "Weighted Round Robin". Below this is a table with two columns: "Queue" and "Weights".

Queue	Weights
1	1
2	2
3	4
4	8

Below the table is a "Save Settings" button. The browser's address bar at the bottom shows "Connecting to 71.6.38.185..." and the IP address "71.6.38.185".

**DSCP** can be implemented on this page. There are eight queues available numbering 0 – 7. Click on the Mode selector to choose DSCP. Then settings will be available to assign DHCP codes to the eight queues.

IP Precedence	Assigned Queue
00	0
01	0
02	1
03	1
04	2
05	2
06	3
07	3

**802.1P** priority is supported to four queues. Each priority level can be assigned to one of the four queues.

The screenshot shows a web-based configuration interface for a network device. The left sidebar contains a menu with the following items: Setup, System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS (highlighted in yellow), SNMP, LLDP, Admin, Statistics, Help, and Logout. The main content area is titled "802.1P" and includes a breadcrumb trail: Queue Settings | DSCP | 802.1P | Port-based QoS | Rate Control | DSCP Remark. Below the breadcrumb, there are two dropdown menus: "802.1P Priority" set to 0 and "Assigned Queue" set to 1. There are "Change" and "Save Settings" buttons. A table below shows the mapping of priority levels to queue numbers:

Priority	Queue
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

The browser address bar at the bottom shows "https://71.6.38.185/cos.htm" and the IP address "71.6.38.185".



**Port-based QoS** allows the priority for each port to be manually set. Click the Update button when done to save changes.

Setup | Queue Settings | DSCP | 802.1P | **Port-based QoS** | Rate Control | DSCP Remark |

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
Security  
**QoS**  
SNMP  
LLDP  
Admin  
Statistics  
Help  
Logout

Change Priority : Port  Priority

Port	Priority	Port	Priority
01	0	25	0
02	0	26	0
03	0	27	0
04	0	28	0
05	0	29	0
06	0	30	0
07	0	31	0
08	0	32	0
09	0	33	0
10	0	34	0
11	0	35	0
12	0	36	0
13	0	37	0
14	0	38	0
15	0	39	0
16	0	40	0

Done 71.6.38.185

**Rate Control** allows traffic shaping for each port. An ingress rate limit can also be set.

The screenshot shows the 'Rate Control' configuration page. The left sidebar contains a 'Setup' menu with options: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS (highlighted), SNMP, LLDP, Admin, Statistics, Help, and Logout. The main content area has a breadcrumb trail: Queue Settings | DSCP | 802.1P | Port-based QoS | Rate Control | DSCP Remark. The configuration fields are: Port (01), Ingress Rate (No Limit), Egress Traffic Shaping (Disabled), Rate (No Limit), Tokens Added Per Interval (2 Tokens), Token Update Interval (7.8125 us (Each token represents 0.5 bit)), and Burst Size (64 Kbits). There are 'Save Settings' and 'Show Rate Table' buttons at the bottom. The status bar at the bottom shows 'Done' and the IP address '71.6.38.185'.

The screenshot shows the 'DSCP Remark' configuration page. The left sidebar is the same as in the previous screenshot, with 'QoS' highlighted. The breadcrumb trail is: Queue Settings | DSCP | 802.1P | Port-based QoS | Rate Control | DSCP Remark. The configuration fields are: ACL Entry Name (dropdown), New DSCP Value (No Change), and buttons for 'Change' and 'Save Settings'. Below these fields is a table with two columns: 'ACL Entry Name' and 'New DSCP Value'. The status bar at the bottom is partially visible.

## 10.9 SNMP

Various screens are available to enable and manipulate SNMP. Profiles can be set for users, communities, and groups. SNMP allows network managers to obtain specific performance and configuration information from a software agent on a remote-network device. SNMP allows different types of networks to communicate by exchanging network information through messages known as protocol data units (PDUs). The IntraCore IC3724PWR supports SNMPv1, v2 and v3. The SNMPv3 protocol has improved the authentication, access control, and security methods

Use the following screens to set the read/write access and to enable or disable the trap authentication for this switch. The default SNMP read community access is public; the default SNMP write community access is private; the default trap authentication is disable.

You can also set SNMP Traps for specific IP addresses allowing them to have access to communities that is different then the default set for the switch.

The screenshot shows the 'SNMP' configuration page. The left sidebar contains a 'Setup' menu with options: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, **SNMP**, LLDP, Admin, Statistics, Help, and Logout. The main content area has a breadcrumb trail: 'SNMP | Group Profile | User Profile | Community Profile | SNMP Trap Station'. The configuration options are: 'Enable SNMP Functionalities' (checked), 'Enable SNMP Notification' (checked), 'Engine ID' (80 00 07 e5 04), and 'Use Default' (80 00 07 e5 04 00036d101835). A 'Save Settings' button is located below the fields. The browser address bar shows 'https://71.6.38.185/submenu7.htm' and the IP address '71.6.38.185' is visible in the bottom right corner.

The screenshot shows the 'Group Profile' configuration page. The left sidebar is the same as the previous screenshot, with 'SNMP' highlighted. The breadcrumb trail is: 'SNMP | **Group Profile** | User Profile | Community Profile | SNMP Trap Station'. The main content area features a 'Group ID' dropdown menu and a 'Create New Group' button. Below this is a table with the following data:

Group ID	Group Name	SNMP Version	Authentication	Access
1	v1	SNMPv1	Disabled	R W

Below the table are 'Previous Page' and 'Next Page' buttons. The browser address bar shows 'https://71.6.38.185/submenu7.htm' and the IP address '71.6.38.185' is visible in the bottom right corner.

## SNMP Continued

Version: ASTN0.02

**Setup** | SNMP | Group Profile | **User Profile** | Community Profile | SNMP Trap Station

User ID  Add New User

User ID	User Name	Group Name	SNMP Version	Auth Type
1	usr1	v1	SNMPv1	None

Previous Page Next Page

**Setup** | SNMP | Group Profile | User Profile | **Community Profile** | SNMP Trap Station

Community ID  Add New Community

Community ID	Community String	Group Name	Remote Station IP
1	public	v1	192.108.250.109

Previous Page Next Page

**Setup** | SNMP | Group Profile | User Profile | Community Profile | **SNMP Trap Station**

Trap Station ID  Add New Trap Station

Trap Station ID	Community String	Remote IP Address	Link Change Trap	Boot Up Trap	Version
-----------------	------------------	-------------------	------------------	--------------	---------

Previous Page Next Page



## 10.10 LLDP

Setup | **LLDP Settings** | LLDP Statistics | Local Information | Remote Information |

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
Security  
QoS  
SNMP  
**LLDP**  
Admin  
Statistics  
Help  
Logout

LLDP System Settings [Change Settings](#)

LLDP:	Disabled
Advertised Interval (5-32768 sec):	30
Hold value (2-10):	4
Re-initialization Delay (1-10 sec):	2
Transmit Delay (1-8192 sec):	2
Notification Interval (5-3600 sec):	5
MED Device Type:	Not Defined
Fast Start Count(1-10):	3
Management Address Transmit Ports:	

LLDP Port Settings [Change Settings](#)

Select	Port	LLDP State	SNMP Notification	MED Fast Start Notification	Optional Enabled TLVs			
					Basic	802.1	802.3	MED
<input type="radio"/>	1	Disabled	Disabled	Disabled	--	--	--	--
<input type="radio"/>	2	Disabled	Disabled	Disabled	--	--	--	--
<input type="radio"/>	3	Disabled	Disabled	Disabled	--	--	--	--
<input type="radio"/>	4	Disabled	Disabled	Disabled	--	--	--	--

Done 71.6.38.185

Setup | LLDP Settings | **LLDP Statistics** | Local Information | Remote Information |

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
Security  
QoS  
SNMP  
**LLDP**  
Admin  
Statistics  
Help  
Logout

Number of Inserts:	N/A
Number of Deletes:	N/A
Number of Drops:	N/A
Number of Ageouts:	N/A

Port	TX Frames	RX Frames Discarded	RX Frames Errors	RX Frames Total	RX Frames TLVs Discarded	RX Frames TLVs Unrecognized	RX Frames Ageouts
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Done 71.6.38.185

Version : ASTN0.02

**Setup** | LLDP Settings | LLDP Statistics | **Local Information** | Remote Information

- System
- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP**
- Admin
- Statistics
- Help
- Logout

<b>Chassis ID SubType</b>					N/A
<b>Chassis ID</b>					N/A
<b>System Name</b>					N/A
<b>System Description</b>					N/A
<b>System Capabilities</b>					N/A
<b>Enabled Capabilities</b>					N/A
<b>MED Device Type</b>					N/A
<b>Management Addresses</b>					
Address Sub-type	Address	Interface Sub-type	Interface Number	OID	
N/A	N/A	N/A	N/A	N/A	N/A

Port	Port ID SubType	Port ID	Port Description
1	N/A	N/A	N/A
2	N/A	N/A	N/A
3	N/A	N/A	N/A
4	N/A	N/A	N/A
5	N/A	N/A	N/A
6	N/A	N/A	N/A
7	N/A	N/A	N/A
8	N/A	N/A	N/A

Done 71.6.38.185

**Setup** | LLDP Settings | LLDP Statistics | Local Information | **Remote Information**

- System
- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP**
- Admin
- Statistics
- Help
- Logout

MSAP Entry	Local Port	Chassis ID SubType	Chassis ID	Port ID SubType	Port ID	Details

## 10.11 Admin - Admin Password

Admin password is the screen that can be used to change the password. Remember to click Save Settings when done.

The screenshot shows the 'Admin Password' configuration page. The left sidebar contains a 'Setup' menu with options: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, LLDP, Admin (highlighted), Statistics, Help, and Logout. The main content area has a top navigation bar with 'Admin Password' selected, and other options: L2 Table, Static Address, Dynamic ARP, Port Mirroring, and Admin Timeout. The configuration fields include 'Old Password', 'New Password', and 'Confirm New Password', each with an input field. A 'Save Settings' button is located below the input fields. The top right corner of the page indicates 'Version: ASTN0.02'.

**L2 Table** makes available MAC addresses and lists the port they are associated with. Aging time can also be specified.

The screenshot shows the 'L2 Table' configuration page. The left sidebar is identical to the previous screenshot, with 'Admin' highlighted. The main content area has a top navigation bar with 'L2 Table' selected. The configuration fields include 'L2 Table Aging Enable' (checked) and 'Aging Time' (set to 300). Below these are 'Reload L2 Table' and 'Clear L2 Table' buttons. A table displays the current L2 entries:

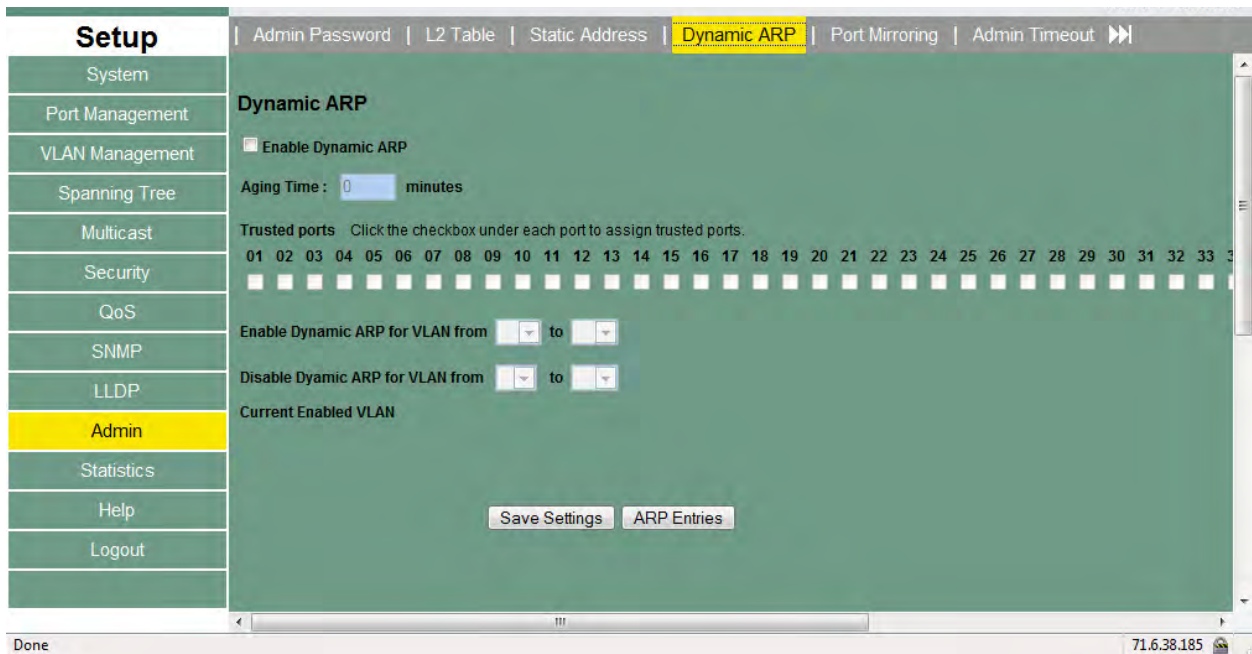
Entry	Source MAC	Port	VLAN ID	Type
0	00-00-94-E0-00-01	34	1	dynamic
1	00-19-21-6D-B4-F6	34	1	dynamic
2	00-0A-27-89-94-A4	34	1	dynamic
3	00-03-93-E4-DF-99	34	1	dynamic
4	00-00-94-D2-E2-A9	34	1	dynamic
5	00-0D-87-95-34-E8	34	1	dynamic

Below the table, it shows 'Total L2 Entries: 6 ( Static: 0 , Dynamic: 6 )'. There are 'Previous Page' and 'Next Page' buttons. At the bottom, there is an 'L2 Entry Lookup' section with input fields for 'MAC' (00-00-00-00-00-00) and 'VLAN ID' (1), and a 'Lookup' button. The bottom status bar shows 'Done' on the left and '71.6.38.185' on the right.

**Static addresses** can be added using this screen.

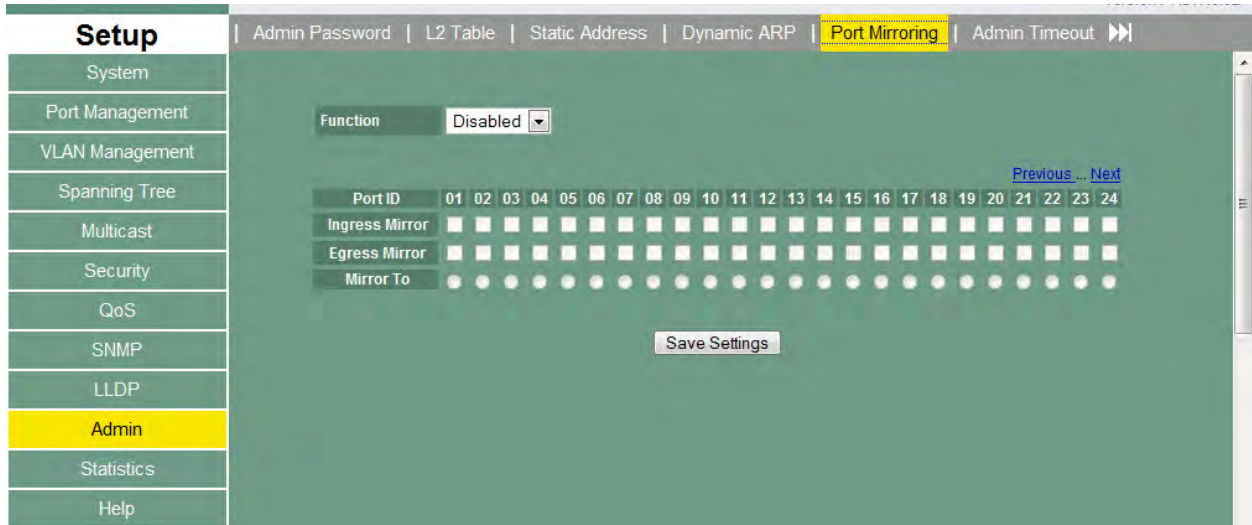


**Dynamic ARP** is the screen that allows aging time and trusted ports to be set on a per port basis. Click Save Setting when done.

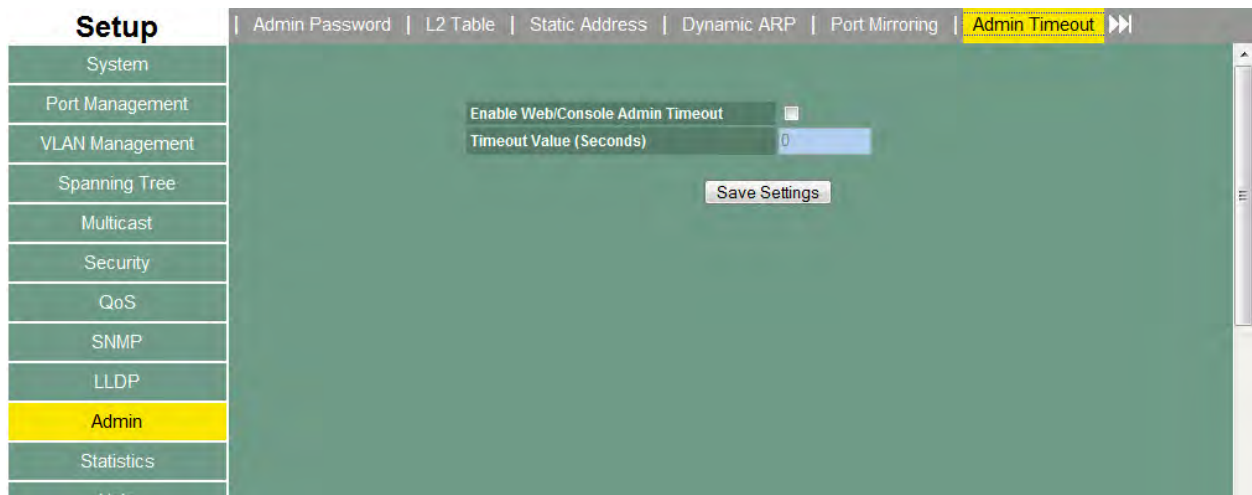




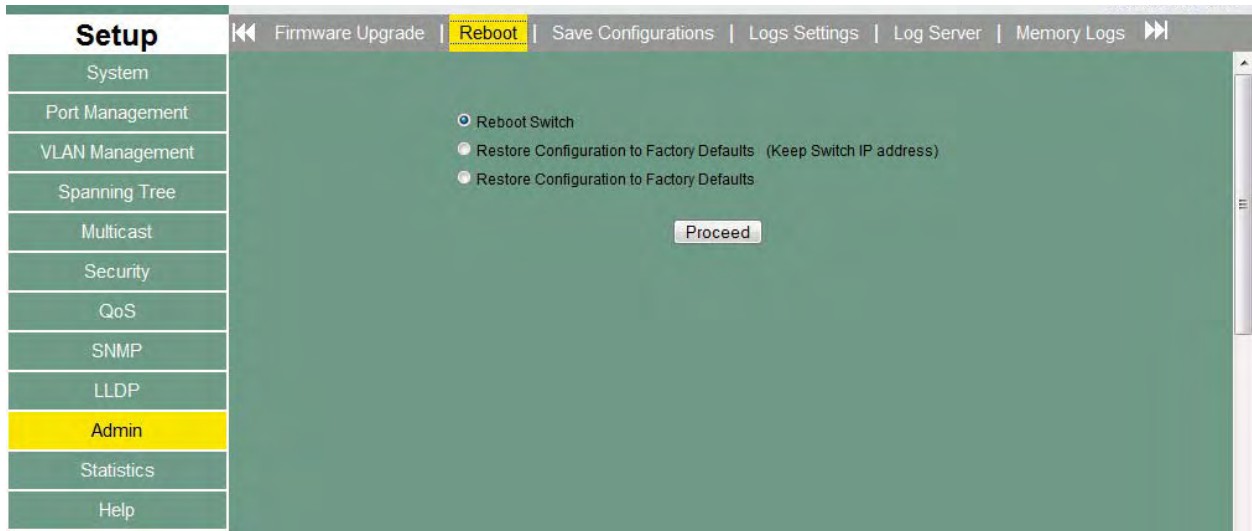
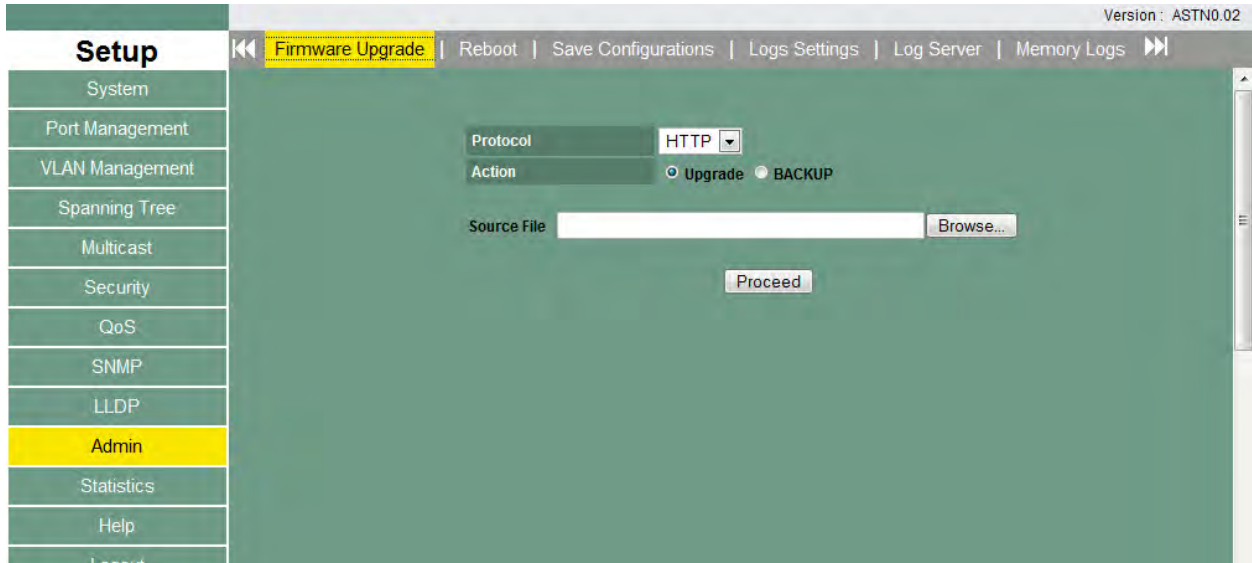
**Port Mirroring** – To set up a mirror, identify the port to be mirrored by checking the ingress mirror, or egress mirror for the port. Next select the port to mirror the information to.



**Admin Timeout** allows the timeout in seconds to be set before the management session is terminated do to no activity.



**ADMIN Continued** – assorted administration functions are controlled using the next several screens.



Setup ◀◀ Firmware Upgrade | Reboot | **Save Configurations** | Logs Settings | Log Server | Memory Logs ▶▶

System

Port Management

VLAN Management

Spanning Tree

Multicast

Security

QoS

SNMP

LLDP

**Admin**

Statistics

Help

Protocol: HTTP

Action:  Upgrade  Backup

Source File:

Setup ◀◀ Firmware Upgrade | Reboot | Save Configurations | **Logs Settings** | Log Server | Memory Logs ▶▶

System

Port Management

VLAN Management

Spanning Tree

Multicast

Security

QoS

SNMP

LLDP

**Admin**

Statistics

Target   Level	ERROR	WARNING	INFO	DEBUG	ACTION
<a href="#">Memory</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">CLEAR</a>
<a href="#">Flash</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">CLEAR</a>
<a href="#">Console</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Version: ASTN0.02

**Setup** ◀◀ Firmware Upgrade | Reboot | Save Configurations | Logs Settings | **Log Server** | Memory Logs ▶▶

- System
- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin**
- Statistics
- Help

Server Name

Server IP Address

Service UDP Port

Facility

**Setup** ◀◀ Firmware Upgrade | Reboot | Save Configurations | Logs Settings | Log Server | **Memory Logs** ▶▶

- System
- Port Management
- VLAN Management
- Spanning Tree
- Multicast
- Security
- QoS
- SNMP
- LLDP
- Admin**
- Statistics
- Help
- Logout

349	INFO	TELNETD	2007/1/8 23:18:21	A telnet client dis-connected from 0.0.0.0
348	INFO	TELNETD	2007/1/8 23:18:18	A telnet client connected from 80.8.83.39
347	INFO	TELNETD	2007/1/8 21:48:47	A telnet client dis-connected from 0.0.0.0
346	INFO	TELNETD	2007/1/8 21:48:46	A telnet client connected from 66.243.208.33
345	INFO	TELNETD	2007/1/8 20:01:15	A telnet client dis-connected from 72.27.17.199
344	INFO	TELNETD	2007/1/8 19:58:14	A telnet client connected from 72.27.17.199
343	INFO	TELNETD	2007/1/8 19:43:02	A telnet client dis-connected from 0.0.0.0
342	INFO	TELNETD	2007/1/8 19:42:48	A telnet client connected from 93.124.2.60
341	INFO	TELNETD	2007/1/8 12:47:59	A telnet client dis-connected from 0.0.0.0
340	INFO	TELNETD	2007/1/8 12:47:57	A telnet client connected from 88.73.117.220
339	INFO	TELNETD	2007/1/8 4:06:41	A telnet client dis-connected from 0.0.0.0
338	INFO	TELNETD	2007/1/8 4:06:40	A telnet client connected from 217.44.230.198
337	INFO	TELNETD	2007/1/8 1:00:10	A telnet client dis-connected from 72.27.149.31
336	INFO	TELNETD	2007/1/8 1:00:05	A telnet client connected from 72.27.149.31
335	INFO	TELNETD	2007/1/7 8:09:53	A telnet client dis-connected from 0.0.0.0

Waiting for 71.6.38.185... 71.6.38.185



**Setup** | Flash Logs | Ping Function | Cable Diagnostic | DHCP Relay | DHCP Option 82

System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
Security  
QoS  
SNMP  
LLDP  
**Admin**  
Statistics  
Help  
Logout

Page 1 of 7 Goto page [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#) [Next](#)

Index	Level	Category	Time	Message
322	ERROR	None	2007/ 1/ 1 2:51:20	ERROR: port 0:ge24: timeout draining packets (325 cells remain)
321	ERROR	None	2007/ 1/ 1 0:50:41	ERROR: port 0:ge22: timeout draining packets (322 cells remain)
320	ERROR	None	2007/ 1/ 2 18:21:00	ERROR: port 0:ge40: timeout draining packets (326 cells remain)
319	ERROR	None	2007/ 1/ 1 1:02:53	ERROR: port 0:ge40: timeout draining packets (187 cells remain)
318	ERROR	None	2007/ 1/ 1 0:15:32	ERROR: port 0:ge42: timeout draining packets (31 cells remain)
317	ERROR	None	2007/ 1/ 1 0:14:05	ERROR: port 0:ge36: timeout draining packets (88 cells remain)
316	ERROR	None	2007/ 1/ 1 0:12:56	ERROR: port 0:ge36: timeout draining packets (59 cells remain)
315	ERROR	None	2007/ 1/ 1 0:12:52	ERROR: port 0:ge36: timeout draining packets (59 cells remain)
314	ERROR	None	2007/ 1/ 1 0:10:34	ERROR: port 0:ge40: timeout draining packets (187 cells remain)
313	ERROR	None	2007/ 1/ 1 0:09:22	ERROR: port 0:ge36: timeout draining packets (6 cells remain)
312	ERROR	None	2007/ 1/ 1 0:08:52	ERROR: port 0:ge40: timeout draining packets (161 cells remain)
311	ERROR	None	2007/ 1/ 1 0:02:13	ERROR: port 0:ge38: timeout draining packets (10 cells remain)

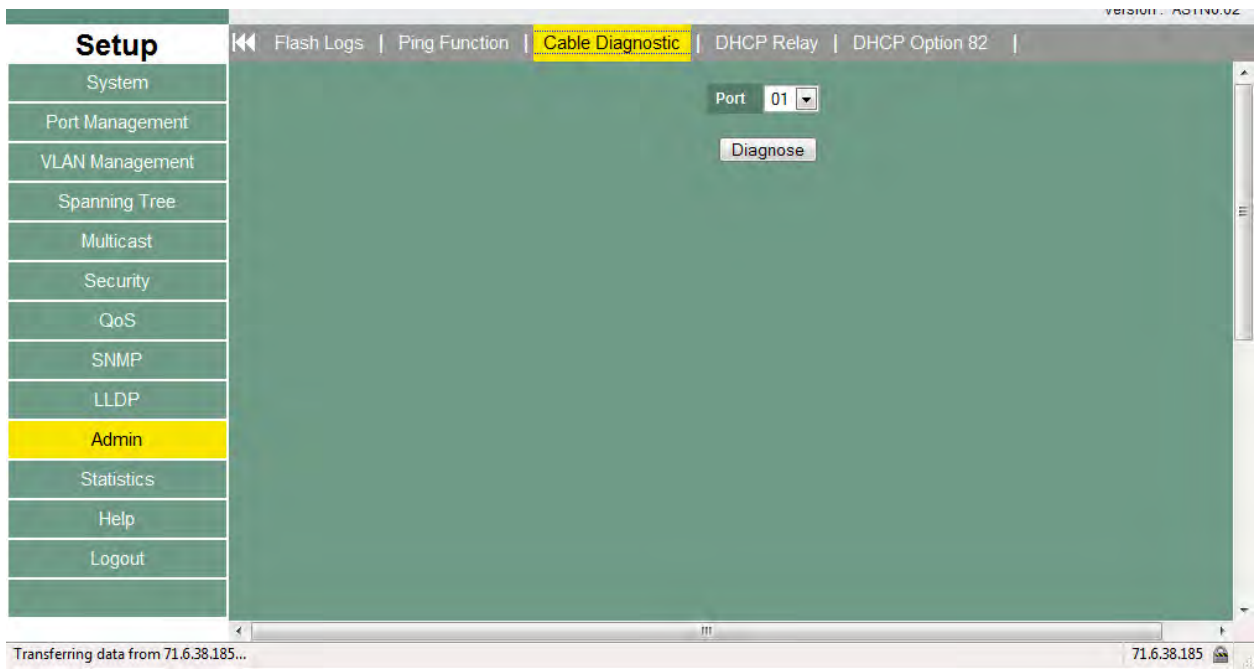
Done 71.6.38.185

**Setup** | Flash Logs | **Ping Function** | Cable Diagnostic | DHCP Relay | DHCP Option 82

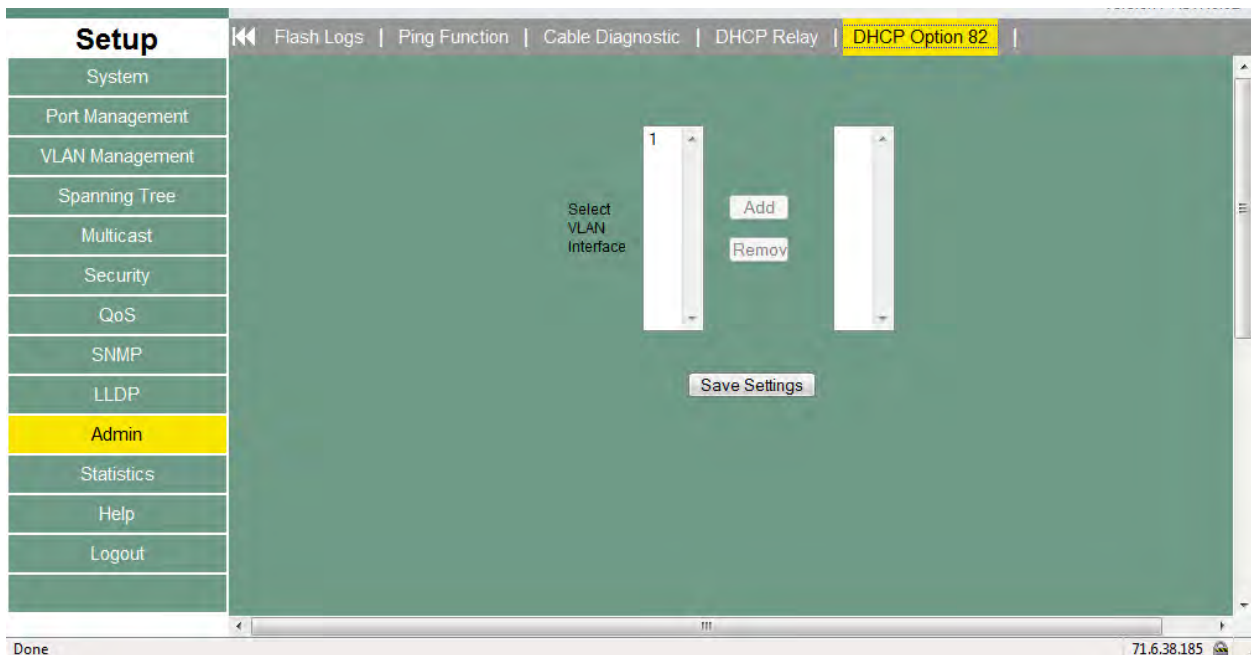
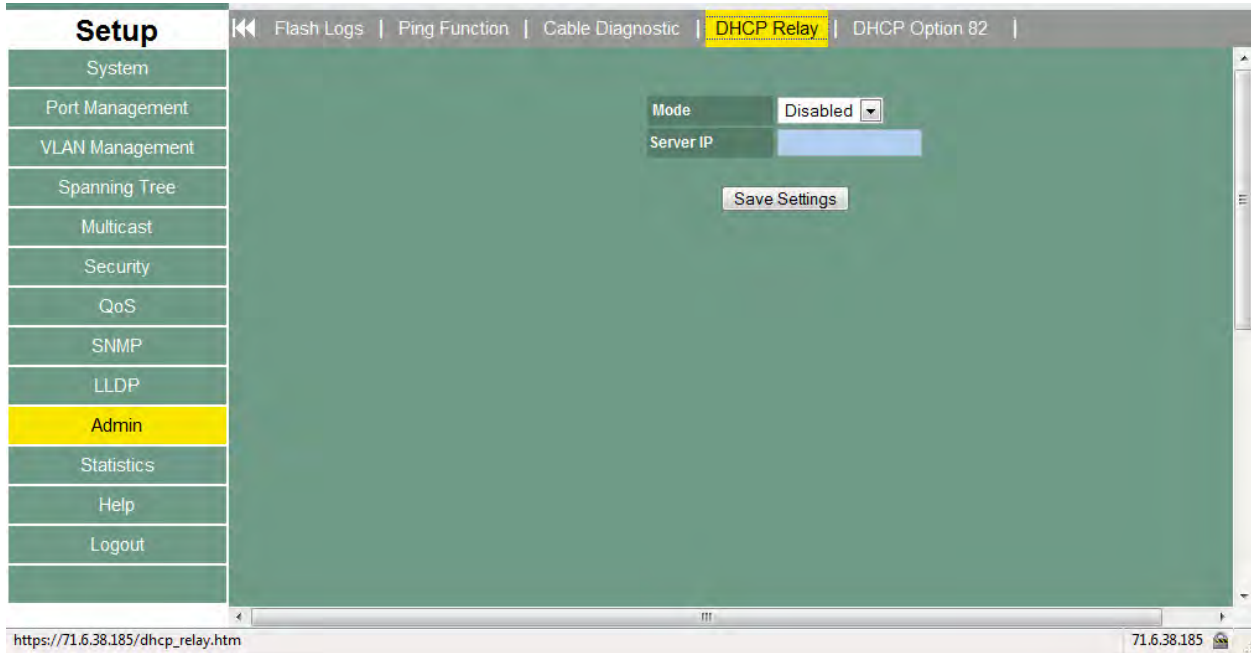
System  
Port Management  
VLAN Management  
Spanning Tree  
Multicast  
Security  
QoS  
SNMP  
LLDP  
**Admin**  
Statistics

Host IP Address

**Cable diagnostic** a cable test that can be run for each port.



**DHCP Relay/ DCP Option 82** – these screens control the relay of DHCP information from a server. VLANs can also be specified to receive DHCP information.



## 10.12 Statistics

RMON information and settings are controlled using the next screens. General counters and timers are also displayed.

Setup		802.1X Statistic	RMON Statistic	RMON Event	RMON Event Log	RMON Alarm	RMON History
System	Port	Octet Received	Octet Transmitted	Session Time	Terminate Cause	User Name	
Port Management	01	0	0	0	0	N/A	
VLAN Management	02	0	0	0	0	N/A	
Spanning Tree	03	0	0	0	0	N/A	
Multicast	04	0	0	0	0	N/A	
Security	05	0	0	0	0	N/A	
QoS	06	0	0	0	0	N/A	
SNMP	07	0	0	0	0	N/A	
LLDP	08	0	0	0	0	N/A	
Admin	09	0	0	0	0	N/A	
Statistics	10	0	0	0	0	N/A	
Help	11	0	0	0	0	N/A	
Logout	12	0	0	0	0	N/A	
	13	0	0	0	0	N/A	
	14	0	0	0	0	N/A	
	15	0	0	0	0	N/A	
	16	0	0	0	0	N/A	
	17	0	0	0	0	N/A	
	18	0	0	0	0	N/A	
	19	0	0	0	0	N/A	
	20	0	0	0	0	N/A	



Version : ASTN0.02

**Setup** | 802.1X Statistic | **RMON Statistic** | RMON Event | RMON Event Log | RMON Alarm | RMON History

Source Interface	Owner	Status
01	monitor	Disabled
02	monitor	Disabled
03	monitor	Disabled
04	monitor	Disabled
05	monitor	Disabled
06	monitor	Disabled
07	monitor	Disabled
08	monitor	Disabled
09	monitor	Disabled
10	monitor	Disabled
11	monitor	Disabled
12	monitor	Disabled
13	monitor	Disabled
14	monitor	Disabled
15	monitor	Disabled
16	monitor	Disabled
17	monitor	Disabled
18	monitor	Disabled
19	monitor	Disabled
20	monitor	Disabled
21	monitor	Disabled
22	monitor	Disabled

Left sidebar menu: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, LLDP, Admin, **Statistics**, Help, Logout

Version : ASTN0.02

**Setup** | 802.1X Statistic | RMON Statistic | **RMON Event** | RMON Event Log | RMON Alarm | RMON History

Index: 1

Description:

Event Type:  None  Log  SNMP-Trap  Log and Trap

Community:

Owner:

Left sidebar menu: System, Port Management, VLAN Management, Spanning Tree, Multicast, Security, QoS, SNMP, LLDP, Admin, **Statistics**, Help

**Setup** | 802.1X Statistic | RMON Statistic | RMON Event | **RMON Event Log** | RMON Alarm | RMON History

System

Port Management

VLAN Management

Spanning Tree

Multicast

Security

QoS

SNMP

LLDP

Admin

**Statistics**

Help

Index	Event Type	Last Time Sent	Owner
<input type="button" value="Refresh"/>			

**Setup** | 802.1X Statistic | RMON Statistic | RMON Event | RMON Event Log | **RMON Alarm** | RMON History

System

Port Management

VLAN Management

Spanning Tree

Multicast

Security

QoS

SNMP

LLDP

Admin

**Statistics**

Help

Logout

Index	1
Interval(Second)	0
Source Interface	(Unassigned)
Variable	(Unassigned)
Sample Type	Absolute
Startup Alarm	Rising Threshold
Rising Threshold	0
Falling Threshold	0
Rising Event	0:None(Unassigned)
Falling Event	0:None(Unassigned)
Owner	

Done 71.6.38.185

**Setup** | 802.1X Statistic | RMON Statistic | RMON Event | RMON Event Log | RMON Alarm | **RMON History**

System  
 Port Management  
 VLAN Management  
 Spanning Tree  
 Multicast  
 Security  
 QoS  
 SNMP  
 LLDP  
 Admin  
**Statistics**  
 Help  
 Logout

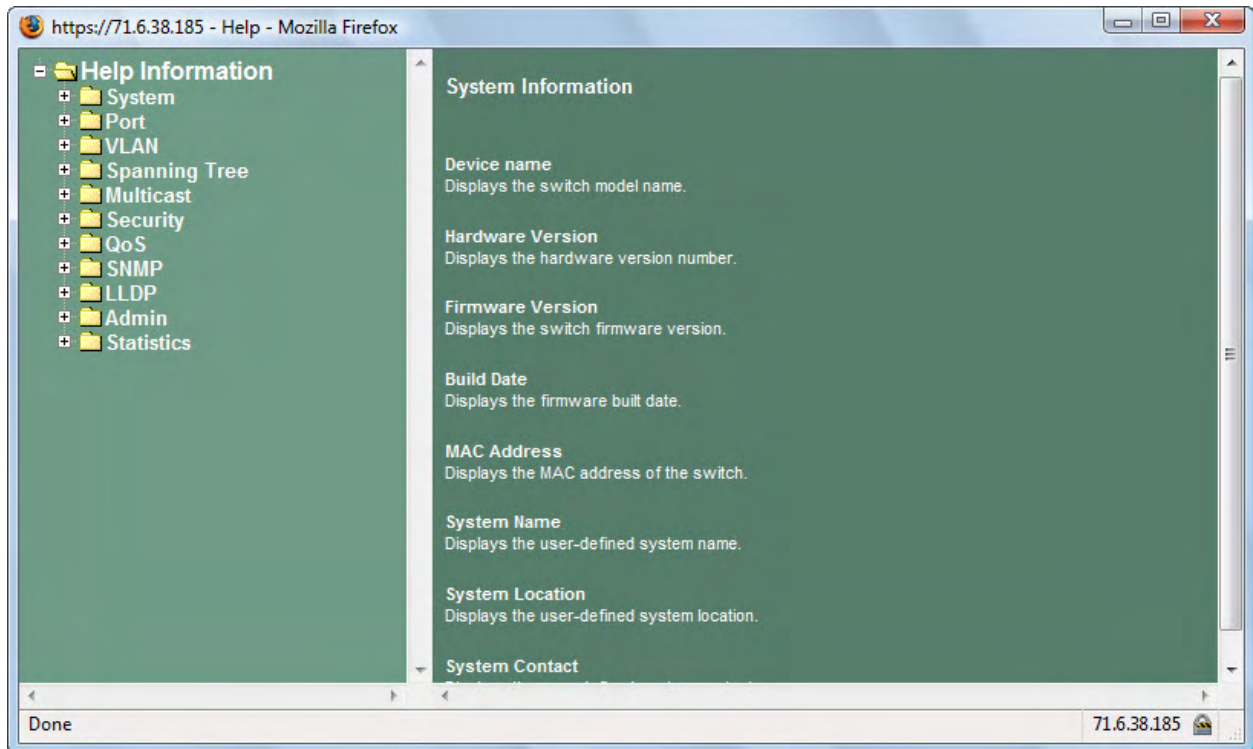
Control Index

Index	Source Interface	Sampling Requested	Current Number of Samples	Sampling Interval	Owner	Status
<a href="#">1</a>	01	50	50	1800	monitor	Disabled
<a href="#">2</a>	02	50	50	1800	monitor	Disabled
<a href="#">3</a>	03	50	50	1800	monitor	Disabled
<a href="#">4</a>	04	50	50	1800	monitor	Disabled
<a href="#">5</a>	05	50	50	1800	monitor	Disabled
<a href="#">6</a>	06	50	50	1800	monitor	Disabled
<a href="#">7</a>	07	50	50	1800	monitor	Disabled
<a href="#">8</a>	08	50	50	1800	monitor	Disabled
<a href="#">9</a>	09	50	50	1800	monitor	Disabled
<a href="#">10</a>	10	50	50	1800	monitor	Disabled
<a href="#">11</a>	11	50	50	1800	monitor	Disabled
<a href="#">12</a>	12	50	50	1800	monitor	Disabled
<a href="#">13</a>	13	50	50	1800	monitor	Disabled
<a href="#">14</a>	14	50	50	1800	monitor	Disabled
<a href="#">15</a>	15	50	50	1800	monitor	Disabled
<a href="#">16</a>	16	50	50	1800	monitor	Disabled
<a href="#">17</a>	17	50	50	1800	monitor	Disabled
<a href="#">18</a>	18	50	50	1800	monitor	Disabled
<a href="#">19</a>	19	50	50	1800	monitor	Disabled

Connecting to 71.6.38.185... | 71.6.38.185

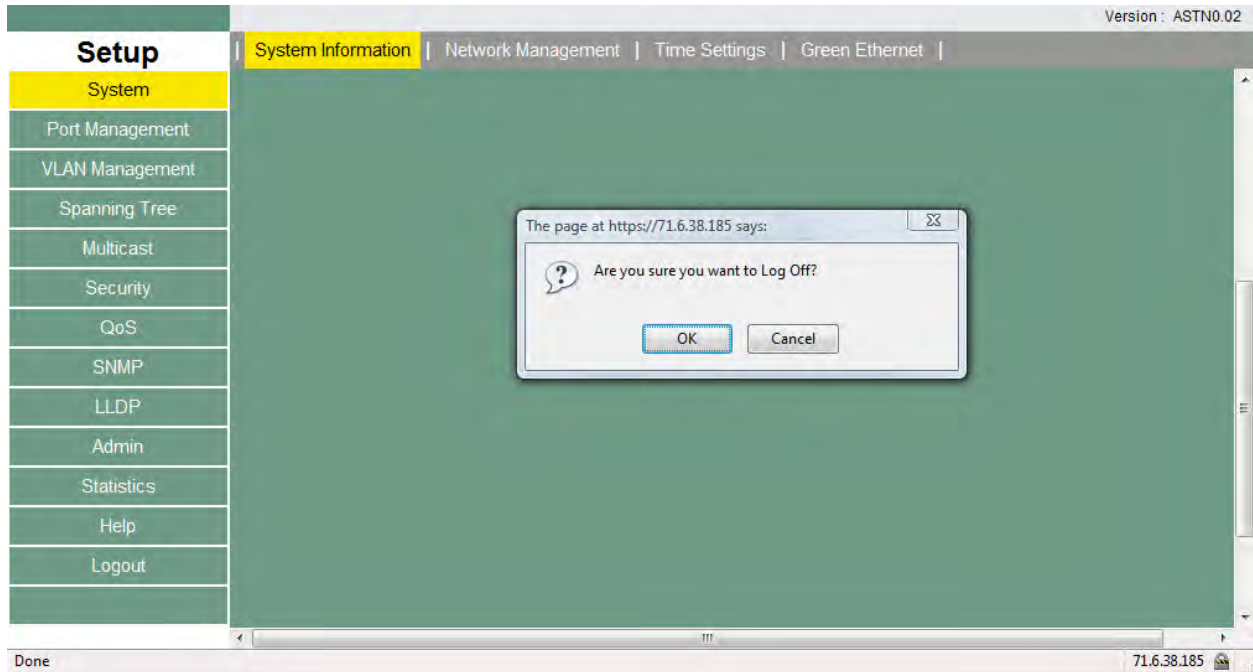
## 10.13 Help

General help is available for many screens.



## 10.14 Logout

Use this screen to logout and close the session.



## Chapter 11: CLI Commands

### Command Modes

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

#### User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is: **Command Prompt: COMMAND>**

#### Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

**Command Prompt: Switch#**

#### Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is: **Command Prompt: Switch(Config)#**

From the Global Config mode, the operator may enter the following configuration mode:

#### Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface. In this mode, a physical port is set up for a specific logical connection operation. The command prompt at this level is: **Command Prompt: Switch(Interface <port#>)#**

## 11.1 User Mode commands

### 11.1.1 Help

This command displays help information

**Format** help

**Mode** User Mode

### 11.1.2 ?

This command displays help information

**Format** help

**Mode** User Mode

### 11.1.3 logout

This command is used to exit from the telnet

**Format** logout

**Mode** User Mode

### 11.1.4 ping

This command sends echo messages.

**Format** ping <A.B.C.D>

**Mode** User Mode

### 11.1.5 show

#### 1) *show port*

This command displays port status.

**Format** show port {<port#> | all}

**Mode** User Mode

#### 2 ) *show network*

This command displays switch IP configuration

**Format** show network

**Mode** User Mode

#### 3) *show system*

This command displays system information.

**Format** show system

**Mode** User Mode

#### 4) *show port statistics*

This command displays port statistics.

**Format** show port statistics {<port#> | all}

**Mode** User Mode

### 11.1.6 enable

Enter to the Privileged Mode

**Format** enable

**Mode** User Mode

## 11.2 Privileged Mode commands

### 11.2.1 cable-diag

This command is used to proceed cable diagnostic

**Format** cable-diag port <port ID>

**Mode** Privileged Mode

e.g. Switch#cable-diag port 1

### 11.2.1 clear

#### 11.2.2.1 clear arl

This command is used to clear ARL table entries

**Format** clear arl

**Mode** Privileged Mode

#### 1) clear arl dynamic

This command is used to Clear dynamic arl table entries

**Format** clear arl dynamic

**Mode** Privileged Mode

#### 2) clear arl static

This command is used to clear static arl table entries

**Format** clear arl static mac <mac-addr>

**Mode** Privileged Mode

### 11.2.2.2 clear config

This command is used to restore switch factory default configuration

**Format** clear config

**Mode** Privileged Mode

### 11.2.2.3 clear counters

This command is used to clear RMON statistics for entire switch

**Format** clear counters

**Mode** Privileged Mode

### 11.2.2.4 clear IGMPsnooping

This command is used to restore igmpsnooping configuration to factory default

**Format** clear igmpsnooping

**Mode** Privileged Mode

### 11.2.2.5 clear static-mcast

This command is used to clear static multicast groups

**Format** clear static-mcast

**Mode** Privileged Mode

### 11.2.2.6 clear pass

This command is used to restore administrator's password to factory default

**Format** clear pass

**Mode** Privileged Mode

### 11.2.2.7 clear lacp

This command is used to restore LAG and LACP configuration to factory default

**Format** clear lacp

**Mode** Privileged Mode

### 11.2.2.8 clear logs

This command is used to clear memory/flash logs

**Format** clear logs

**Mode** Privileged Mode

### 11.2.2.9 clear VLAN

This command is used to delete all VLAN groups

**Format** clear vlan

**Mode** Privileged Mode

## 11.2.3 configuration



Enter into Global Configuration mode

**Format** configuration

**Mode** Privileged Mode

#### **11.2.4 copy**

This command is used to upload file from switch to host, or download file to switch from host

##### **11.2.4.1 copy nvram\_config**

This command is used to backup switch configuration

**Format** copy nvram\_config tftp <A.B.C.D> file <filename>

**Mode** Privileged Mode

e.g. Switch#copy nvram\_config tftp 192.168.1.100 file switch\_configuration

##### **11.2.4.2 copy system\_image**

This command is used to backup switch runtime image

**Format** copy system\_image tftp <A.B.C.D> <filename>

**Mode** Privileged Mode

e.g. Switch#copy system\_image tftp 192.168.1.100 image\_file

##### **11.2.4.3 copy tftp**

This command is used to upload configuration or runtime image

**Format** copy tftp <A.B.C.D> file <filename> {nvram\_config | system\_image}

**Mode** Privileged Mode

e.g. Switch#copy tftp 192.168.1.100 file switch\_configuration nvram\_config

Switch#copy tftp 192.168.1.100 file runtime\_code system\_image

##### **11.2.5 exit**

This command is used to exit current shell

**Format** exit

**Mode** Privileged Mode

##### **11.2.6 help**

This command displays help information

**Format** help

**Mode** Privileged Mode

##### **11.2.7 logout**

This command is used to exit current shell

**Format** logout

**Mode** Privileged Mode

##### **11.2.8 ping**

This command is used to proceed ping destination host

**Format** ping <A.B.C.D>

**Mode** Privileged Mode

##### **11.2.9 reload**

This command is used to reboot system

**Format** reload

**Mode** Privileged Mode

##### **11.2.10 save**

This command is used to save configuration

**Format** save

**Mode** Privileged Mode

##### **11.2.11 show**

This command is used to show configured data

###### **11.2.11.1 show qos**

This command display class of service information

###### **1) show qos cos**

This command display the cos mapping

**Format** show qos cos

**Mode** Privileged Mode

###### **2) show qos queue-settings**

This command display the queue-settings mapping

**Format** show qos queue-settings

**Mode** Privileged Mode

**3) show qos advanced**

This command display qos advanced mode information

**show qos advanced mode**

This command display mode of qos

**Format** show qos advanced mode

**Mode** Privileged Mode

**show qos advanced dscp**

This command display qos dscp mapping

**Format** show qos advanced dscp

**Mode** Privileged Mode

**show qos advanced ip-precedence**

This command display qos ip precedence mapping

**Format** show qos advanced ip-precedence

**Mode** Privileged Mode

**4) show qos port-based**

This command is used to display class of service information

**show qos port-based port**

This command display class of service information

**Format** show qos port-based port <port-ID>

**Mode** Privileged Mode

**show qos port-based all**

This command display all switch interfaces' cos settings

**Format** show qos port-based all

**Mode** Privileged Mode

**11.2.11.2 show dot1x**

This command display dot1x information

**1) show dot1x config**

This command display dot1x and port configuration

**Format** show dot1x config

**Mode** Privileged Mode

**2) show dot1x radius**

This command display radius configuration

**Format** show dot1x radius

**Mode** Privileged Mode

**3) show dot1x statistics**

This command display dot1x statistics

**Format** show dot1x statistics

**Mode** Privileged Mode

**11.2.11.3 show igmp snooping**

This command display IGMP snooping information

**1) show igmp snooping dynamic\_router\_port**

This command display dynamic router ports information

**Format** show *igmp* snooping dynamic\_router\_port

**Mode** Privileged Mode

**2) show IGMP snooping groups**

This command is used to display *igmp* groups information

**Format** show IGMP snooping groups

**Mode** Privileged Mode

**11.2.11.4 show interface**

This command is used to display summary statistics

**1) show interface history**

This command is used to display port RX and TX

**Format** show interface history <port-ID>

**Mode** Privileged Mode

## **2) show interface statistics**

This command is used to display port summary statistics

**Format** show interface statistics <port-ID>

**Mode** Privileged Mode

### **11.2.11.5 show lag**

This command is used to display link aggregation groups information

#### **1) show lag lag-index**

This command is used to specify an switch lag

**Format** show lag lag-index <port-ID>

**Mode** Privileged Mode

#### **2) show lag all**

This command is used to display all switch lag

**Format** show lag all <port-ID>

**Mode** Privileged Mode

### **11.2.11.6 show lldp**

This command is use to display lldp statistics

#### **1) show lldp statistic**

This command is used to display lldp statistic

**Format** show lldp statistic

**Mode** Privileged Mode

#### **2) show lldp local**

This command is used to display local information

**Format** show lldp local

**Mode** Privileged Mode

#### **3) show lldp msap**

This command is used to display msap information

**Format** show lldp msap

**Mode** Privileged Mode

#### **4) show lldp msap-entry**

This command is used to display msap details information

**Format** show lldp msap-entry <1..26>

**Mode** Privileged Mode

### **11.2.11.7 show logging**

This command is used to display trap records

#### **1) show logging memory-log**

This command display memory log

**Format** show logging memory-log

**Mode** Privileged Mode

#### **2) show logging flash-log**

This command display flash logs

**Format** show logging flash-log

**Mode** Privileged Mode

### **11.2.11.8 show monitor**

This command is used to display port mirroring settings

**Format** show monitor

**Mode** Privileged Mode

### **11.2.11.9 show network**

This command is used to configuration for inband connectivity

**Format** show network

**Mode** Privileged Mode

### **11.2.11.10 show port**

This command is used to display port mode and settings, display port status

#### **1) show port port-index**

This command is used to specify an switch interface

**Format** show port port-index <port-ID>

**Mode** Privileged Mode

### ***show port all***

This command is used to display all switch interface

**Format** show port all

**Mode** Privileged Mode

### **11.2.11.11 show port-security**

This command is used to display port security settings

#### **1) show port-security port**

This command is used to specify an switch interface

**Format** show port-security port <port-ID>

**Mode** Privileged Mode

#### **2) show port-security all**

This command is used to display all interfaces' status

**Format** show port-security all

**Mode** Privileged Mode

### **11.2.11.12 show rate-limit**

This command is used to ingress and egress rate limit information

#### **1) show rate-limit port**

This command is used to specify an switch interface

**Format** show rate-limit port <port-ID>

**Mode** Privileged Mode

e.g. Switch#Show rate-limit port 1

Switch#Show rate-limit port g1

#### **2) show rate-limit all**

This command is used to display all interfaces' status

**Format** show Rate-Limit all

**Mode** Privileged Mode

### **11.2.11.13 show running-config**

This command is used to display switch running config

**Format** show running-config

**Mode** Privileged Mode

### **11.2.11.14 show snmp**

This command is used to display all snmp config

#### **1) show snmp groups**

This command display all snmp groups

**Format** show snmp groups

**Mode** Privileged Mode

#### **2) show snmp users**

This command display all snmp users

**Format** show snmp users

**Mode** Privileged Mode

#### **3) show snmp communities**

This command display all snmp communities

**Format** show snmp communities

**Mode** Privileged Mode

### **11.2.11.15 show snmp**

This command is used to display switch snmp information

**Format** show snmp

**Mode** Privileged Mode

### **11.2.11.16 show spanning-tree**

This command displays Spanning Tree information

#### **1) show spanning-tree interface**

This command displays RSTP ports information

**show spanning-tree interface port**

This command specify an switch interface

**Format** show spanning-tree interface port<port-ID>

**Mode** Privileged Mode

**show spanning-tree interface all**

This command display all switch interface

**Format** show spanning-tree interface all

**Mode** Privileged Mode

**2) show spanning-tree mst**

This command display MST information

**show spanning-tree mst detailed**

This command display a MST instance information

**Format** show spanning-tree mst detailed <0..4094>

**Mode** Privileged Mode

**show spanning-tree mst instance**

This command display ports information on a MST instance

**Format** show spanning-tree mst instance <0..4094>

**Mode** Privileged Mode

**show spanning-tree mst summary**

This command display all MST instance information

**Format** show spanning-tree mst summary

**Mode** Privileged Mode

**show spanning-tree status**

This command is used to display spanning-tree status

**Format** show Spanning-tree status

**Mode** Privileged Mode

**11.2.11.17 show storm-control**

This command is used to display storm-control information

**Format** show storm-control

**Mode** Privileged Mode

**11.2.11.18 show sysinfo**

This command is used to display system information including system up time

**Format** show sysinfo

**Mode** Privileged Mode

**11.2.11.19 show switch**

This command is used to display switch information

**1) show switch admin-time**

This command display the age time of web and console

**Format** show switch admin-time

**Mode** Privileged Mode

**2) show switch age-time**

This command display the age time of L2 table

**Format** show switch age-time

**Mode** Privileged Mode

**3) show switch mac-table**

This command is used to display address resolution protocol cache

**Format** show switch mac-table

**Mode** Privileged Mode

**4) show switch mcast-table**

This command display multicast address table

**Format** show switch mcast-table

**Mode** Privileged Mode

**11.2.11.20 show trapflags**

This command is used to display the value of trap flags that apply to the switch

**Format** show trapflags

**Mode** Privileged Mode

**11.2.11.21 show vlan**

This command is used to display vlan configuration

**1) show vlan member**

This command display vlan configuration

**Format** show vlan member <1..4094>

**Mode** Privileged Mode

**2)show vlan number**

This command display how many vlan has been created

**Format** show vlan number

**Mode** Privileged Mode

**11.2.11.22 show rmon**

**1) Show rmon event**

**2) Show rmon event Index**

This command displays rmon Event.

**Format** Show rmon event index <1..65535>

**Mode** Privileged Mode

**3) Show rmon event**

**Format** Show rmon event<CR>

**Mode** Privileged Mode

**4) Show rmon Event log**

This command displays rmon event log.

**Format** Show rmon Event log event index <1..65535>

**Mode** Privileged Mode

**5) Show rmon alarm**

**Show rmon alarm index**

This command displays rmon Alarm.

**Format** Show rmon alarm index <1..65535>

**Mode** Privileged Mode

**Show rmon alarm**

**Format** Show rmon alarm<CR>

**Mode** Privileged Mode

**Show rmon event log**

This command displays rmon event log.

**Format** Show rmon event log event index <1..65535>

**Mode** Privileged Mode

**6) Show rmon history**

This command displays rmon history.

**Format** Show rmon history index <1..65535>

**Mode** Privileged Mode

**7)Show rmon statistics**

This command displays port rmon statistics.

**Format** Show rmon statistics

**Mode** Privileged Mode

**11.2.12 telnet**

This command telnet the other host.

**Format** telnet <A.B.C.D>

**Mode** Privileged Mode

## 11.3 Global Config mode commands

### 11.3.1 exit

This command is used to exit current shell

**Format** exit

**Mode** Global Config

### 11.3.2 vlan

This command is used to configure vlan

#### 11.3.2.1 vlan add

This command is used to create a new vlan

**vlan add number**

This command enter a vlan ID

**Format** vlan add number <vlan-ID>

**Mode** Global Config

**vlan add range**

This command enter a range of vlan ID

**Format** vlan add range from < vlan-ID > to <vlan-ID>

**Mode** Global Config

#### 11.3.2.2 vlan delete

This command remove a existed vlan

**Format** vlan delete <vlan-ID>

**Mode** Global Config

#### 11.3.2.3 vlan ingress

This command performs ingress vlan source port membership check

**vlan ingress forward**

The command is used to forward frame but don't learn SA into ARL table

**Format** vlan ingress forward

**Mode** Global Config

**vlan ingress drop**

This command is used to drop frames violation vid

**Format** vlan ingress drop

**Mode** Global Config

**vlan ingress bypass**

This command is used to forward frame and learn SA into ARL table

**Format** vlan ingress bypass

**Mode** Global Config

#### 11.3.2.4 vlan port

This command is used to configure 802.1Q port parameters for vlans

##### 1) **vlan port all**

This command is used to configure all ports

**vlan port all port-configure**

This command is used to configure ports in a specific vlan

**Format** vlan port all port configure <vlan-ID>

**Mode** Global Config

**vlan port all protected**

This command is used to configure protected ports

**Format** vlan port all protected {enable|disable}

**Mode** Global Config

**vlan port all pvid**

This command is used to configure port pvid

**Format** vlan port all pvid <vlan-ID>

**Mode** Global Config

##### 2) **vlan port ports**

This command is used to configure multiple ports

**vlan port ports port-configure**

This command is used to configure ports in a specific vlan

**Format** vlan port ports port-configure <vlan-ID>

**Mode** Global Config

#### **vlan port ports protected**

This command is used to configure protected ports

**Format** vlan port ports protected {enable|disable}

**Mode** Global Config

#### **vlan port ports pvid**

This command is used to configure port vid

**Format** vlan port ports pvid < vlan-ID>

**Mode** Global Config

### **11.3.2.5 vlan lag**

This command is used to configure lag to a special vlan

#### **1) vlan lag vlan < vlan-id> exclude**

This command is used to remove lag from a vlan

**Format** vlan lag vlan < vlan-ID> exclude lags <lag-ID>

**Mode** Global Config

#### **2) vlan lag vlan <vlan-ID> untagged**

This command is used to set to untagged lag.

**Format** vlan lag vlan <vlan-ID> untagged lags <lag-ID>

**Mode** Global Config

#### **3) vlan lag vlan <vlan-ID> tagged**

This command is used to set to tagged lag.

**Format** vlan lag vlan <vlan-ID> tagged lags <lag-ID>

**Mode** Global Config

### **11.3.3 Bridge**

This command is used to configure switch aging time

**Format** bridge aging-time <0-1048575>

**Mode** Global Config

### **11.3.4 lacp-syspri**

This command is used to configure lacp system priority

**Format** lacp-syspri system-priority <0-65535>

**Mode** Global Config

### **11.3.5 link-aggregation**

This command is used to configure link aggregation

#### **11.3.5.1 link-aggregation addport**

This command is used to configure LAG groups

**Format** Link Aggregation addport lag <LAG-ID>

**Mode** Global Config

#### **11.3.5.2 link aggregation delport**

This command remove ports from LAG

##### **1) Link Aggregation delport all**

This command remove all ports from a LAG

**Format** link-aggregation-delport all lag <LAG-ID>

**Mode** Global Config

##### **2) link aggregation delport lag**

This command remove specify LAG group

**Format** link aggregation delport lag <LAG-ID>

**Mode** Global Config

### **11.3.6 LLDP**

#### **11.3.6.1 lldp enable**

This command is used to enable lldp functions

**Format** lldp enable

**Mode** Global Config

#### **11.3.6.2 lldp disable**



This command is used to disable lldp functions

**Format** lldp disable

**Mode** Global Config

### 11.3.6.3 lldp adv-interval

This command is used to specify advertised interval in seconds

**Format** lldp adv-interval <5-32768>

**Mode** Global Config

### 11.3.6.4 lldp fast-startcnt

This command is used to specify advertised interval in seconds

**Format** lldp fast-startcnt <1-10>

**Mode** Global Config

### 11.3.6.5 lldp hold

This command is used to specify hold value

**Format** lldp hold <2-10>

**Mode** Global Config

### 11.3.6.6 lldp notify-interval

This command is used to specify notification interval in seconds

**Format** lldp notify-interval <5-3600>

**Mode** Global Config

### 11.3.6.7 lldp reinit-delay

This command is used to specify re-initialization delay in seconds

**Format** lldp reinit-delay <1-10>

**Mode** Global Config

### 11.3.6.8 lldp tx-delay

Transmit Delay in seconds

**Format** lldp tx-delay <1-8192>

**Mode** Global Config

### 11.3.6.9 lldp mgmt-addrtxport

A range of ports can be set.

**Format** lldp mgmt-addrtxport ports <port list>

**Mode** Global Config

e.g. switch(config)# lldp mgmt-addrtxport ports 1

switch(config)# lldp mgmt-addrtxport ports 1-4

## 11.3.7 Log

This command is used to configure log server

### 11.3.7.1 Log log-server

This command is used to configure log server

#### 1) Log log-server name <WORD>add

This command is used to specify log server name, enter a name, up to 12 characters, add a log server IP address

**Format** Log log-server name <WORD> add ipaddr word

**Mode** Global Config

#### 2) Log log-server name <word> delete

This command is used to delete a log server

**Format** log log-server name <WORD> delete

**Mode** Global Config

### 11.3.7.2 Log logging-target

This command is used to configure log notification level

#### 1) log logging-target memory

This command is used to specify memory log notify-level

**Format** log logging-target memory {enable|disable}

**Mode** Global Config

#### 2) log logging-target flash

This command is used to specify flash log notify-level

**Format** log logging-target flash {enable|disable}

**Mode** Privileged Mode

### **3) log logging-target console**

This command is used to specify console log notify-level

**Format** log logging-target console {enable|disable}

**Mode** Global Config

### **4) log logging-target server**

This command is used to specify console log notify-level

**Format** log logging-target server name <WORD> {enable|disable}

**Mode** Global Config

### **11.3.8 radius-server**

This command is used to configure radius server

**Format** radius-server ip <IP addr>

**Mode** Global Config

### **11.3.9 static-address**

This command is used to specify static address

#### **11.3.9.1 static-address add**

This command is used to add static mac address

**Format** static-address add <mac addr> vid <vlan-ID> port <port-ID>

**Mode** Global Config

#### **11.3.9.2 static-address delete**

This command is used to delete static mac address

**Format** static-address delete <mac addr> vid <vlan-ID>

**Mode** Global Config

### **11.3.10 mgmt-accesslist commands**

#### **11.3.10.1 mgmt-accesslist ipaddr**

This command specifies a management access IP for the DUT, up to 8 IP address can be set.

**Format** mgmt-accesslist ipaddr <IP addr>

**Mode** Global Config

#### **11.3.10.2 mgmt-accesslist enable**

This command enables management access list. Only the IP address specified in the management list is allowed to access DUT.

**Format** mgmt-accesslist enable

**Mode** Global Config

#### **11.3.10.3 mgmt-accesslist disable**

This command disables management access list.

**Format** mgmt-accesslist disable

**Mode** Global Config

### **11.3.11 monitor commands**

#### **11.3.11.1 monitor enable**

This command enables port mirroring.

**Format** monitor enable

**Mode** Global Config

#### **11.3.11.2 monitor disable**

This command disables port mirroring.

**Format** monitor disable

**Mode** Global Config

#### **11.3.11.3 monitor des**

Configure destination port.

##### **1) monitor des <port-ID> probetype bidirection**

This command configures port monitor probetype as bi-direction traffic.

**Format** monitor des <port-ID> probetype bidirection src <port list>

**Mode** Global Config

e.g. Switch(config)# monitor des 1 probetype bidirection src 2-8

##### **2) monitor des <port-ID> probetype ingress**

This command configures port monitor probetype as ingress traffic.

**Format** monitor des <port-ID> probetype ingress src <port list>

**Mode Global Config**

e.g. Switch(config)# monitor des 1 probetype ingress src 2-8

**3) monitor des <port-ID> probetype egress**

This command configures port monitor probetype as egress traffic.

**Format** monitor des <port-ID> probetype egress src <port list>

**Mode Global Config**

e.g. Switch(config)# monitor des 1 probetype egress src 2-8

**11.3.12 dot1x commands**

**11.3.12.1 dot1x enable**

This command enables global 802.1x function.

**Format** dot1x enable

**Mode Global Config**

**11.3.12.2 dot1x disable**

This command disables global 802.1x function.

**Format** dot1x disable

**Mode Global Config**

**11.3.12.3 dot1x port-control**

Configure port auto-authentication mode.

**1) dot1x port-control enable**

This command set auto-authorized on a list of ports.

**Format** dot1x port-control enable port <port list>

**Mode Global Config**

**2) dot1x port-control disable**

This command set force authorized on a list of ports.

**Format** dot1x port-control disable port <port list>

**Mode Global Config**

e.g. Switch(config)# dot1x port-control disable port 1-4

**11.3.13 network commands**

**11.3.13.1 network mgmt-vlan**

This command changes management vlan.

**Format** network mgmt-vlan <vlan-ID>

**Mode Global Config**

**11.3.13.2 network parms**

This command configures static IP address of the switch.

**Format** network parms <IP addr> <subnet mask> <gateway>

**Mode Global Config**

**11.3.13.3 network protocol**

This command configure switch dhcp client.

**Format** network protocol {dhcp|none}

**Mode Global Config**

**11.3.13.4 network dhcp-relay**

Configure switch dhcp relay functions.

**1) network dhcp-relay mode**

This command configures dhcp relay mode.

**Format** network dhcp-relay mode {enable|disable}

**Mode Global Config**

**2) network dhcp-relay server**

This command configures dhcp-relay server ip-address.

**Format** network dhcp-relay server <A.B.C.D>

**Mode Global Config**

**3) network dhcp-relay vlan**

Configure dhcp-relay option-82 vlan information.

**network dhcp-relay vlan <vlan-ID> add**

This command enters a vlan which will be enable DHCP-relay option82.

**Format** network dhcp-relay vlan <vlan-ID> add

**Mode Global Config**

**network dhcp-relay vlan <vlan-ID> remove**

This command enters a vlan which will be disable dhcp-relay option82.

**Format** network dhcp-relay vlan <vlan-ID> remove

**Mode** Global Config

**11.3.13.5 network sysinfo**

Configure switch system information.

**Network sysinfo sysname**

This command configures system name.

**Format** network sysinfo sysname <WORD>

**Mode** Global Config

**network sysinfo syslocate**

This command configures system location.

**Format** network sysinfo syslocate <WORD>

**Mode** Global Config

**network sysinfo syscontact**

This command configures system contact information.

**Format** network sysinfo syscontact <WORD>

**Mode** Global Config

**11.3.13.6 network admin-timeout**

This command configures web/console admin time out interval.

'0' means disable.

**Format** network admin-timeout <0-65535>

**Mode** Global Config

**11.3.14 port-all commands****11.3.14.1 port-all admin-mode**

This command configures ports admin mode.

**Format** port-all admin-mode {enable | disable}

**Mode** Global Config

**11.3.14.2 port-all auto-negotiate**

This command configures ports auto-negotiation mode.

**Format** port-all auto-negotiate {enable|disable}

**Mode** Global Config

**11.3.14.3 port-all flow-control**

This command configures ports flow control.

**Format** port-all flow-control {enable|disable}

**Mode** Global Config

**11.3.14.4 port-all portsec-lockmode**

Configure port security.

**1) port-all portsec-lockmode none**

This command disable port security.

**Format** port-all portsec-lockmode none

**Mode** Global Config

**2) port-all portsec-lockmode static**

*Note:* This commands only support on G24-PORTS 100BASETX + 2 GIGABIT COMBO PORTS LAYER 2 MANAGEMENT SWITCHL/ G48 100BASETX + 4 GIGABIT COMBO WITH 2 SHARED MINI-GBIC SLOTS LAYER 2+ MANAGEMENT SWITCH.

This command enable static lock mode.

**Format** port-all portsec-lockmode static

**Mode** Global Config

**3) port-all portsec-lockmode dynamic**

This command enable limited dynamic lock mode.

**Format** port-all portsec-lockmode dynamic max-entries <0-24>

**Mode** Global Config

**11.3.14.5 port-all rate-limit**

Configure rate limit value on all ports.

### **1)port-all rate-limit egress**

This command specifies egress rate limit.

**Format** port-all Rate-Limit egress <value>

**Mode** Global Config

### **2)port-all rate-limit ingress**

This command specifies ingress rate limit.

**Format** port-all rate-limit ingress <value>

**Mode** Global Config

### **11.3.14.6 port-all rmon-counter**

This command configures rmon counter capability on ports.

**Format** port-all rmon-counter {enable|disable}

**Mode** Global Config

### **11.3.14.7 port-all speed**

This command configures ports speed.

**Format** port-all speed {10hd|10fd|100hd|100fd}

**Mode** Global Config

### **11.3.14.8 port-all storm-control**

Configure all ports' storm control settings.

#### **1) port-all storm-control disable**

This command disables storm control.

**Format** port-all Storm-Control disable

**Mode** Global Config

#### **2) port-all storm-control broadcast**

This command configures storm control for broadcast only.

**Format** port-all storm-control broadcast <value>

**Mode** Global Config

#### **3) port-all storm-control broadcast-multicast**

This command configures storm control for broadcast and multicast.

**Format** port-all Storm-Control broadcast-multicast <value>

**Mode** Global Config

#### **4) port-all storm-control broadcast-unknown**

This command configures storm control for broadcast and unknown unicast.

**Format** port-all storm-control broadcast-unknown <value>

**Mode** Global Config

#### **5) port-all storm-control all-cast**

This command configures storm control for broadcast, multicast and unknown unicast.

**Format** port-all Storm-Control all-cast <value>

**Mode** Global Config

### **11.3.15 qos commands**

#### **11.3.15.1 qos qos-advanced**

Configure qos advanced mode.

##### **1) qos qos-advanced DSCP**

This command enables DSCP mode.

**Format** qos qos-advanced DSCP

**Mode** Global Config

##### **2) qos qos-advanced ip\_precedence**

This command enables IP Precedence mode.

**Format** qos qos-advanced ip\_precedence

**Mode** Global Config

##### **3) qos qos-advanced none**

This command disables qos advanced mode.

**Format** qos qos-advanced none

**Mode** Global Config

#### **11.3.15.2 qos cos**

This command configures 802.1p priority queue mapping.

**Format** Qos cos priority <0-7> queue <1-4>

**Mode** Global Config

#### **11.3.15.3 qos dscp**

This command specifies dscp value to queue mapping.

**Format** Qos dscp <0-63> queue <1-4>

**Mode** Global Config

#### **11.3.15.4 qos port-based**

This command configures port-based priority mapping.

**Format** qos port-based port <WORD>status {enable | disable}

**Mode** Global Config

#### **11.3.15.5 qos scheduling**

Configure qos scheduling mode.

##### **1) qos scheduling strict**

This command sets to strict priority.

**Format** qos scheduling strict

**Mode** Global Config

##### **2) qos scheduling wrr**

This command sets to Weight Round-Robin.

**Format** qos scheduling wrr

**Mode** Global Config

#### **11.3.15.6 qos ip-precedence**

This command configures IP precedence queue mapping.

**Format** qos ip-precedence <0-7> queue <1-4>

**Mode** Global Config

#### **11.3.15.7 qos wrr**

This command configures queue weight for weight round robin.

**Format** qos wrr weight <1-15> queue <1-4>

**Mode** Global Config

### **11.3.16 set commands**

#### **11.3.16.1 set IGMP**

Configure IGMP snooping.

##### **1) set igmp enable**

This command enables igmp snooping.

**Format** set igmp enable

**Mode** Global Config

##### **2) set igmp disable**

This command disables IGMP snooping.

**Format** set igmp disable

**Mode** Global Config

##### **3) set igmp last-memberquery**

This command specifies last member query interval.

**Format** set igmp last-memberquery <1-200>

**Mode** Global Config

##### **4) set igmp last-membercount**

This command specifies last member count.

**Format** set igmp last-membercount <1-20>

**Mode** Global Config

##### **5) set igmp query-interval**

This command specifies igmp query interval<secs>.

**Format** set igmp query-interval <10-600>

**Mode** Global Config

##### **6) set igmp query-resinterval**

This command specifies igmp query response interval<secs>.

**Format** set igmp query-resinterval <0-200>

**Mode** Global Config

##### **7) set igmp robustness**

This command specifies robustness variable.

**Format** set igmp robustness <1-20>

**Mode** Global Config

### **8) set igmp router-port**

This command specifies igmp router port.

**Format** set igmp router-port ports <port list>

**Mode** Global Config

e.g. Switch(config)# set igmp router-port ports 1-10

### **11.3.16.2 set igmp-querier**

This command configures igmp querier.

**Format** set igmp-querier {enable | disable}

**Mode** Global Config

### **11.3.16.3 set igmp-proxy**

This command configures igmp proxy.

**Format** set igmp-proxy {enable | disable}

**Mode** Global Config

### **11.3.16.4 set static-mcast**

Configure static multicast.

#### **1) set static-mcast name <WORD> add**

This command create a multicast group.

**Format** set static-mcast name <WORD> add vid <vlan-ID> mac <mac-addr>member port <port list>

**Mode** Global Config

#### **2) set static-mcast name <WORD>delete**

This command delete a static multicast group.

**Format** set static-mcast name <WORD>delete

**Mode** Global Config

## **11.3.17 snmp commands**

### **11.3.17.1 snmp notify**

This command configures snmp notification.

**Format** snmp notify {enable|disable}

**Mode** Global Config

### **11.3.17.2 snmp group**

#### **1) snmp group add**

This command create a snmp group.

**Format** snmp group add <WORD>version <1-2>

**Mode** Global Config

#### **2) snmp group delete**

This command delete a snmp group.

**Format** snmp group delete <WORD>

**Mode** Global Config

### **11.3.17.3 snmp user**

#### **1) snmp user add**

This command creates a snmp user.

**Format** snmp user add <user name> group <group name> version <1-3>

**Mode** Global Config

#### **2) snmp user delete**

This command deletes a snmp user.

**Format** snmp user delete <WORD>

**Mode** Global Config

### **11.3.17.4 snmp community**

#### **1) snmp community add**

This command creates a community.

**Format** snmp community add <community name> group <group name> mgmt-ip <ip-addr>

**Mode** Global Config

## **2) snmp community delete**

This command deletes a community.

**Format** snmp community delete <community name>.

**Mode** Global Config

### **11.3.17.5 snmp trapstation**

#### **1) snmp trapstation add**

Create a snmp trap station.

**snmp trapstation add <ip-addr> community <community name> type bootup**

Send trap when system reboot

**Format** snmp trapstation add <ip-addr> community <community name> type bootup trap-version {1|2}

**Mode** Global Config

**snmp trapstation add <ip-addr> community <community name> type linkchange**

Send trap when port link change.

**Format** snmp trapstation add <ip-addr> community <community name> type linkchange trap-version {1|2}

**Mode** Global Config

**snmp trapstation add <ip-addr> community <community name> type both**

Send trap when system reboot or port link change.

**Format** snmp trapstation add <ip-addr> community <community name> type both trap-version {1-2}

**Mode** Global Config

**snmp trapstation add <ip-addr> community <community name> type none**

Send no trap.

**Format** snmp trapstation add <ip-addr> community <community name> type none trap-version {1-2}

**Mode** Global Config

#### **2) snmp trapstation delete**

This command delete a trap station.

**Format** snmp trapstation delete <WORD>

**Mode** Global Config

### **11.3.18 sntp commands**

#### **11.3.18.1 sntp daylight**

This command enables or disables the daylight saving configuration.

**Format** sntp daylight {enable|disable}

**Mode** Global Config

#### **11.3.18.2 sntp localtime**

Configure the local time.

##### **1) sntp localtime enable**

This command enables local time.

**Format** sntp localtime enable

**Mode** Global Config

##### **2) sntp localtime localtime\_date**

This command sets local time.

**Format** sntp localtime localtime\_date <year> <month> <date> <hour> <minute> <second>

**Mode** Global Config

#### **11.3.18.3 sntp server**

##### **1) sntp server enable**

This command enables sntp server.

**Format** sntp server enable

**Mode** Global Config



## **2) snmp server ipaddr**

This command sets snmp server IP address.

**Format** snmp server ipaddr <IP-addr>

**Mode** Global Config

## **3) snmp server polling**

This command sets snmp server polling time interval.

**Format** snmp server polling <0-9>

**Mode** Global Config

## **11.3.18.4 snmp timezone**

This command sets snmp timezone.

**Format** snmp timezone <1-75>

**Mode** Global Config

## **11.3.19 spanning-tree commands**

### **11.3.19.1 spanning-tree forceversion**

This command configures Spanning Tree protocol version.

#### **1) spanning-tree forceversion 8021s**

This command selects spanning tree type as 8021.s(multiple Spanning Tree).

**Format** spanning-tree forceversion 8021s

**Mode** Global Config

#### **2) spanning-tree forceversion 8021w**

This command selects spanning tree type as 802.1w(rapid Spanning Tree).

**Format** spanning-tree forceversion 8021w

**Mode** Global Config

#### **3) spanning-tree forceversion none**

This command selects none spanning tree type.

**Format** spanning-tree forceversion none

**Mode** Global Config

### **11.3.19.2 spanning-tree configuration**

This command configures MSTP region name and revision.

#### **1) spanning-tree configuration name**

This command configures MSTP region name (Max.32 chars).

**Format** spanning-tree configuration name <WORD>

**Mode** Global Config

#### **2) spanning-tree configuration revision**

This command configures revision level.

**Format** spanning-tree configuration revision <0-65535>

**Mode** Global Config

### **11.3.19.3 spanning-tree forward-time**

This configures the bridge forward delay parameter.

**Format** spanning-tree forward-time <4-30>

**Mode** Global Config

### **11.3.19.4 spanning-tree max-age**

This command configures the bridge max age parameter.

**Format** spanning-tree max-age <6-40>

**Mode** Global Config

### **11.3.19.5 spanning-tree max-hops**

This command configure the number of hops in a region.

**Format** spanning-tree max-hops <1-40>

**Mode** Global Config

### **11.3.19.6 spanning-tree port**

#### **1)spanning-tree port all**

This command specifies RSTP capability for all ports.

**Format** spanning-tree port all {enable |disable}

**Mode** Global Config

#### **2)spanning-tree port cost**

This command configures RSTP port path cost.

**Format** spanning-tree port cost <0-200000000>

**Mode** Global Config

### **3)spanning-tree port priority**

This command configures RSTP port priority.

**Format** spanning-tree port priority <0-24>

**Mode** Global Config

### **4)spanning-tree port edge**

This command configures STP edge .

**Format** spanning-tree port edge {enable|disable}

**Mode** Global Config

### **5)spanning-tree port force-p2plink**

This command configures force point to point link mode on ports.

**Format** spanning-tree port force-p2plink {auto|enable|disable}

**Mode** Global Config

### **6)spanning-tree port migration-check**

This command Re-checks the appropriate BPDU format to send on ports.

**Format** spanning-tree port migration-check {enable|disable}

**Mode** Global Config

### **11.3.19.7 spanning-tree priority**

This command configures RSTP bridge priority value.

**Format** spanning-tree priority <0-61440>

**Mode** Global Config

### **11.3.19.8 spanning-tree mst**

Configure a multiple spanning tree instance.

#### **1) spanning-tree mst instance**

This command creates or removes a MST instance

##### **spanning-tree mst instance add**

This command creates a MST instance.

**Format** spanning-tree mst instance add vlan <vlan list> mstpid <MST ID>

**Mode** Global Config

e.g. Switch(Config)# Spanning-Tree mst instance add vlan 2-5 mstpid 2

Switch(Config)# Spanning-Tree mst instance add vlan 6 mstpid 3

##### **spanning-tree mst instance delete**

This command removes the last MST instance.

**Format** spanning-tree mst instance delete

**Mode** Global Config

#### **2 )spanning-tree mst vlan**

This command adds or deletes vlan from a MSTP instance.

**spanning-tree mst vlan <MST ID> <vlan list> add**

This command creates a MST instance.

**Format** spanning-tree mst vlan <MST ID> <vlan list> add

**Mode** Global Config

e.g. Switch(Config)# Spanning-Tree mst vlan 3 3-5 add

**Spanning-Tree mst vlan <MST ID> <vlan list> delete**

This command deletes a vlan from a MST instance.

**Format** Spanning-Tree mst vlan <MST ID> < vlan list> delete

**Mode** Global Config

#### **3) spanning-tree mst bridgepri**

This command configures bridge priority for a MST instance.

**Format** spanning-tree mst bridgepri <MST ID> <priority>

**Mode** Global Config

#### **4) spanning-tree mst cost**

This command configures port path cost in a MST instance.

**Format** spanning-tree mst cost <MST ID> <path cost> ports <port list>

**Mode** Global Config

#### **5)spanning-tree mst priority**

This command configures port priority in a MST instance

**Format** spanning-tree mst priority <MST ID> <priority> ports <port list>

**Mode** Global Config

### 11.3.20 User commands

This command changes user password.

**Format** user password

**Mode** Global Config

### 11.3.21 Interface commands

This command enters into configure interface mode.

**Format** Interface <port-ID>

**Mode** Global Config

### 11.3.22 rmon

This command is used to configure RMON.

#### 11.3.22.1 rmon event

This command creates rmon event entry.

**Format** rmon event index < 1..65535 > desc <WORD> event <1..4>  
community <WORD>owner<WORD>

**Mode** Global Config

e.g. Switch(Config)# rmon event index 1 desc 123 event 4 community 123  
owner test

#### 11.3.22.2 rmon alarm

This command creates rmon alarm entry.

**Format** rmon alarm index < 1..65535 >interval<0..3600>interface<port  
number>counter<1..17>sample{absolute|delta}start{rasing|falling|all}rthreshol  
d<0..65535>fthreshold<0..65535> reindex <0..65535> feindex<0..65535>  
owner< WORD>

**Mode** Global Config

e.g. Switch(Config)# RMON alarm index 1 interval 10 interface counter 1  
sample delta start all rthreshold 100 fthreshold 10 reindex 1 feindex 0 owner  
test

#### 11.3.22.3 rmon del

##### 1) rmon del event

This command deletes rmon event entry.

**Format** rmon del event index< 1..65535 >

**Mode** Global Config

##### 2) rmon del alarm

This command deletes rmon alarm entry.

**Format** rmon del alarm index< 1..65535 >

**Mode** Global Config

### 11.3.23 access list commands

*Note:* This commands only support on G24-PORTS 100BASETX + 2 GIGABIT  
COMBO PORTS LAYER 2+ MANAGEMENT SWITCH/G24 GIGABIT PORTS  
WITH 2 SHARED MINI-GBIC SLOTS/G44 GIGABIT PORTS WITH 4  
SHARED MINI-GBIC SLOTS L2 MANAGEMENT SWITCH/G48 100BASETX  
+ 4 GIGABIT COMBO WITH 2 SHARED MINI-GBIC SLOTS LAYER 2+  
MANAGEMENT SWITCH.

#### 11.3.23.1 access-list name <WORD> add

This command creates a new access-list.

**Format** access-list name <WORD> add priority <1-65535>

**Mode** Global Config

#### 11.3.23.2 access-list name <WORD> action

##### 1) access-list name <WORD> action deny

This command denies an ACL entry.

**Format** access-list name <WORD> action deny

**Mode** Global Config

##### 2) access-list name <WORD> action permit

This command permits an ACL entry and queue 1-4 will assign priority queue when rule activated.

**Format** access-list name <WORD> action permit {<cr>|queue <1-4>}

**Mode** Global Config

### 11.3.23.3 access-list name <WORD> clear

This command clears ACL entry contents.

#### 1) access-list name <WORD> clears SRC IP

This command clears the source IP/subnet mask filter.

**Format** access-list name <WORD> clear SRC IP

**Mode** Global Config

#### 2) access-list name <WORD> clears DST IP

This command clears the destination IP/subnet mask filter.

**Format** access-list name <WORD> clear DST IP

**Mode** Global Config

#### 3) access-list name <WORD> clear L4port

**access-list name <WORD> clear L4port SRC port**

This command clears TCP/UDP source port filter.

**Format** access-list name <WORD> clear l4port SRC port

**Mode** Global Config

**access-list name <WORD> clear l4port DST port**

This command clears TCP/UDP destination port filter.

**Format** access-list name <WORD> clear l4port DST port

**Mode** Global Config

#### 4) access-list name <WORD> clear packet-type

This command clears packet type filter.

**Format** access-list name <WORD> clear packet-type

**Mode** Global Config

#### 5) access-list name <WORD> clear mac SA

This command clears a source mac address.

**Format** Access-list name <WORD> clear mac SA

**Mode** Global Config

#### 6) access-list name <WORD> clear MAC DA

This command clears a destination mac address.

**Format** Access-list name <WORD> clear mac DA.

**Mode** Global Config

#### 7)access-list name <WORD> clear VID

This command clears the 802.1Q VLAN tag of packet.

**Format** Access-list name <WORD> clear VID

**Mode** Global Config

#### 8)access-list name <WORD> clear ether-type

This command clears ether type filter.

**Format** access-list name <WORD> clear ether-type

**Mode** Global Config

### 11.3.23.4 access-list name <WORD> deletes.

This command removes the ACL entry.

**Format** access-list name <WORD> deletes

**Mode** Global Config

### 11.3.23.5 access-list name <WORD> {enable|disable}

This command enables/disables the ACL entry.

**Format** access-list name <WORD> {enable|disable}

**Mode** Global Config

### 11.3.23.6 access-list name <WORD> set

#### 1) access-list name <WORD> set priority

This command specifies ACL entry priority.

**Format** access-list name <WORD> set priority <0-65535>

**Mode** Global Config

**2) access-list name <WORD> set IP-mode**

**access-list name <WORD> set IP-mode SRC IP.**

This command specifies a source IP address.

**Format** access-list name <WORD> set IP-mode SRC IP <IP-addr>  
<mask-addr>

**Mode** Global Config

**access-list name <WORD> set IP-mode DST IP**

This command specifies a destination IP address.

**Format** access-list name <WORD> set IP-mode DST IP <IP-addr>  
<mask-addr>

**Mode** Global Config

**3) access-list name <WORD> set L4port**

This command specifies the TCP/UDP port range.

**access-list name <WORD> set L4port SRC-port**

This command specifies the source TCP/UDP port range.

**Format** Access-list name <WORD> set L4 port SRC-port from <1-65535>  
to <1-65535>

**Mode** Global Config

**access-list name <WORD> set L4port DST-port**

This command specifies the destination TCP/UDP port range.

**Format** access-list name <WORD> set L4port DST-port from <1-65535> to  
<1-65535>

**Mode** Global Config

**4) access-list name <WORD> set IP-mode packet-type**

This command specifies the packet type.

**Format** access-list name <WORD> set IP-mode packet-type  
{ICMP|IGMP|IP|TCP|UDP|GRE}

**Mode** Global Config

**5) access-list name <WORD> set mac-mode**

Specify ACL entry priority.

**access-list name <WORD> set mac-mode mac SA**

This command specifies a source mac address.

**Format** Access-list name <WORD> set mac-mode mac SA <mac-addr>  
<mask-addr>

**Mode** Global Config

**access-list name <WORD> set mac-mode mac DA**

This command specifies a destination mac address.

**Format** access-list name <WORD> set mac-mode mac DA <mac-addr>  
<mask-addr>

**Mode** Global Config

**access-list name <WORD> set mac-mode ether-type**

This command specifies the ether type of the packet.

**Format** access-list name <WORD> set mac-mode ether-type  
{ipv4|ARP|xns}

**Mode** Global Config

### 11.3.24 arp Commands

*Note:* This commands only support on GG24 GIGABIT PORTS WITH 2 SHARED MINI-GBIC SLOTS/G44 GIGABIT PORTS WITH 4 SHARED MINI-GBIC SLOTS L2 MANAGEMENT SWITCH)

#### 11.3.24.1 arp dynamic

**1) arp dynamic enables and disables.**

This command enables and disables dynamic arp functions.

**Format** arp dynamic {enable|disable}

**Mode** Global Config

**2) arp dynamic aging-time**

This command set arp dynamic aging-time between 0s and 999s."0"means

disable.

**Format** arp dynamic aging-time <0~999>

**Mode** Global Config

### **3) arp dynamic ports**

This command set dynamic arp ports to trust and un-trust.

**Format** arp dynamic ports {trust|untrust} <port-list>

**Mode** Global Config

e.g. Swtich<Config># arp dynamic ports trust 1-4

Swtich<Config># arp dynamic ports untrust 4

### **4) arp dynamic vlan**

This Command set add/remove dynamic arp on specified vlan.

**Format** arp dynamic vlan {add|remove} from < vlan -id> to < vlan -id>

**Mode** Global Config

e.g. Swtich<Config># arp dynamic vlan add from 1 to 1

Swtich<Config># arp dynamic vlan remove from 1 to 1

### **11.3.24.2 arp static command**

This command set arp static address table for mac address with IP Address.

**Format** arp static {add|delete} vid <1~4094> ip <A.B.C.D> mac <mac-address>

**Mode** Global Config

### **11.3.25 dos Commands**

*Note:* This commands only support on GG24 GIGABIT PORTS WITH 2 SHARED MINI-GBIC SLOTS/G44 GIGABIT PORTS WITH 4 SHARED MINI-GBIC SLOTS L2 MANAGEMENT SWITCH/G48 100BASETX + 4 GIGABIT COMBO WITH 2 SHARED MINI-GBIC SLOTS LAYER 2+ MANAGEMENT SWITCH)

#### **11.3.25.1 dos land**

This Command enables and disables land-type attacks prevention.

**Format** dos land {enable|disable}

**Mode** Global Config

#### **11.3.25.2 dos Blat**

This Command enables and disables blat-type attack prevention.

**Format** dos blat {enable|disable}

**Mode** Global Config

#### **11.3.25.3 dos SYN-fin**

This Command enables and disables SYN-fin-type attack prevention.

**Format** dos syn -fin {enable|disable}

**Mode** Global Config

#### **11.3.25.4 dos ports**

##### **1) dos ports Smurf**

This command enables and disables Smurf-TYPR attack prevention.

**Format** dos ports smurf {enable|disable}

**Mode** Global Config

##### **2)dos ports ping-flooding**

This command enables and disables ping-flooding-type attack prevention.

**Format** dos ports ping-flooding {enable|disable}

**Mode** Global Config

##### **3)dos ports SYNACK-flooding**

This command enables and disables SYNACK -flooding -type attack prevention. Set rate is 64 kbps or 128kbps for port lists (1, 3-5, 7-9.11)

**Format** dos ports synack -flooding {enable|disable} rate {64|128} <port-list>

**Mode** Global Config

e.g. Switch<Config>#dos ports synack -flooding enablerate 64 1-4

Switch<Config>#dos ports synack -flooding enablerate 64 5

## 11.4 Interface Config mode commands

### 11.4.1 exit command

Exit current shell

**Format** exit

**Mode** Interface Config

### 11.4.2 dot1x command

Set 802.1x port control.

#### 11.4.2.1 Set auto-authorized on ports

**Format** 802.1x port-control {enable|disable}

**Mode** Interface Config

### 11.4.3 Configure port lacp mode

#### 11.4.3.1 admin command

Configure admin key of port

**Format** lacp admin <0 ..65535>

**Mode** Interface Config

e.g. switch(interface g1)#lacp admin 36768

#### 11.4.3.2 priority command

Configure lacp port priority

**Format** lacp priority <0..65535>

**Mode** Interface Config

### 11.4.4 addport command

add one port to a LAG group

**Format** addport <LAG-ID>

**Mode** Interface Config

### 11.4.5 delport command

Remove a port from a LAG group

**Format** delport <LAG-ID>

**Mode** Interface Config

### 11.4.6 lldp command

An lldp agent can transmit information about the capabilities and current status of the system associated with its MSAP identifier. The lldp agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, lldp agents are not provided any means of soliciting information from other lldp agents via this protocol.

#### 11.4.6.1 lldp state set

##### *lldp status*

Only transmit the lldp status

**Format** lldp state {tx|rx| tx\_rx|disable}

**Mode** Interface Config

#### 11.4.6.2 configure notifications

Enable/disable notification form the agent

**Format** lldp notification {enable|disable}

**Mode** Interface Config

#### 11.4.6.3 Configure med notifications

Configure whether or not MED notifications from the agent are enabled.

Enable/disable med notification form the agent

**Format** lldp med-notification {enable|disable}

**Mode** Interface Config

e.g. Switch(Interface 1)#lldp med-notification enable

#### 11.4.6.4 Configures which TLVs are enabled for transmission.

##### *1) basic set*

**Format** lldp tlvs-tx {enable|disable} option basic

{port-desc|sys-name|sys-desc|sys-capacity|sys-capacity }

**Mode** Interface Config

#### **2) 8021 set**

Status of local-802.1 settings

**Format** lldp tlvs-tx {enable|disable} option 8021 {pvid| vlanname| protocol-id}

**Mode** Interface Config

eg.switch(interface 1)lldp tlvs enable option 8021 pvid

#### **3) 8023 set**

**Format** lldp tlvs-tx {enable|disable} option 8023 {mac-phy| power| link-aggregation| frame-size}

**Mode** Interface Config

#### **4) MED-set**

Status of MED Settings

**Format** lldp tlvs-tx {enable|disable} option med-set {capabilities| net-policy| location-id| mdi}

**Mode** Interface Config

#### **11.4.7 admin-mode**

Configure administrative mode on a port

**Format** Switch(Interface 1)# admin-mode {enable|disable}

**Mode** Interface Config

#### **11.4.8 auto-negotiate**

Configure auto-negotiate mode on a port

**Format** auto-negotiate {enable|disable}

**Mode** Interface Config

#### **11.4.9 speed**

Set port speed to 10Mbps half duplex/ 10Mbps full/ 100Mbps half/ 100Mbps full/ 1000Mbps 100FX mode/1000base-x full .

**Format** speed {10hd|10fd|100hd|100fd|1000fd|100fx|1000base-x}

**Mode** Interface Config

#### **11.4.10 flow-control command**

##### ***flow-control enable***

This command enable flow-control at port.

**Format** flow-control {enable|disable}

**Mode** Interface Config

#### **11.4.11 port-security command**

##### ***1)port-security***

This command add or delete a static mac into mac security table.

**Format** port-security {add|delete} <sourcemac >

**Mode** Interface Config

##### ***2)port-security lock-mode***

This command enable/disable port security.

**Format** port-security lock-mode {none|static}

**Mode** Interface Config

##### ***port-security lock-mode dynamic***

This command enable limited dynamic lock mode,and specify maximum learning entries for limited dynamic lock mode.the max-entries value :0~25.

**Format** port-security lock-mode dynamic max-entries 24

**Mode** Interface Config

#### **11.4.12 qos command**

This command specifies port-based qos.

**Format** qos port-based status {enable|disable}

**Mode** Interface Config

#### **11.4.13 rate-limit command**

##### ***11.4.13.1 rate-limit Egress***

This command limits egress rate, which the unit is Kbps.



**Format** rate-limit egress *<rate>*

**Mode** Interface Config

#### 11.4.13.2 rate-limit Ingress

This command limits ingress rate, which the unit is Kbps.

**Format** rate-limit ingress *<rate>*

**Mode** Interface Config

#### 11.4.14 storm-control command

##### 11.4.14.1 storm-control

Enable/disable storm control.

**Format** storm-control disable

**Mode** Interface Config

##### 11.4.14.2 storm-control broadcast

This command storm control for broadcast only, and limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

**Format** storm-control broadcast *<rate>*

**Mode** Interface Config

##### 11.4.14.3 storm-control broadcast-multicast

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

**Format** storm-control broadcast-multicast *<rate>*

**Mode** Interface Config

##### 11.4.14.4 storm-control broadcast-unknown

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

**Format** storm-control broadcast-unknown *<rate>*

**Mode** Interface Config

e.g. Switch(Interface 1)# storm-control broadcast-unknown 64

##### 11.4.14.5 storm-control all-cast

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

**Format** storm-control all-cast *<rate>*

**Mode** Interface Config

#### 11.4.15 rmon-counter command

This command specifies rmon counter capability on a port

**Format** rmon-counter {enable|disable}

**Mode** Interface Config

#### 11.4.16 set igmp-router-port command

This command specifies igmp router port .

**Format** set igmp-router-port {enable|disable}

**Mode** Interface Config

#### 11.4.17 spanning-tree command

##### 11.4.17.1 spanning-tree cost

This command configure RSTP port path cost, path cost value:0~200000000.

**Format** spanning-tree cost *<pathcost>*

**Mode** Interface Config

##### 11.4.17.2 spanning-tree edge

This command configure edge property

**Format** spanning-tree edge {enable|disable}

**Mode** Interface Config

e.g. Switch(Interface 1)# spanning-tree edge enable

##### 11.4.17.3 spanning-tree force-p2plink

This command configure force point to point link mode.

**Format** spanning-tree force-p2plink {auto|enable|disable}

**Mode** Interface Config

#### 11.4.17.4 spanning-tree migration-check

This command re-checks the appropriate BPDU format to send on this port

**Format** spanning-tree migration-check {enable|disable}

**Mode** Interface Config

#### 11.4.17.5 spanning-tree mst

This command configures multiple spanning tree instance.

##### 1) *spanning-tree mst cost*

This command configure the path cost on a MST instance :1~200000000.

**Format** spanning-tree mst cost <pathcost>

**Mode** Interface Config

##### 2) *spanning-tree mst priority*

This command configure the port priority on a MST instance:0~4096.

**Format** spanning-tree mst priority <1 4096>

**Mode** Interface Config

#### 11.4.17.6 spanning-tree participation

This command configures RSTP capability on a port.

**Format** spanning-tree participation {enable|disable}

**Mode** Interface Config

#### 11.4.17.7 spanning-tree priority

this command configure RSTP port priority:0~240

**format** spanning-tree priority <0..240>

**mode** Interface Config

#### 11.4.18 VLAN command

##### 11.4.18.1 vlan participation

This command join or leave a vlan.

##### 1) *vlan participation exclude*

This command leave a vlan.

**Format** vlan participation exclude < vlan id>

**Mode** Interface Config

##### 2) *vlan participation*

This command join a vlan with untagged/tagged mode.

**Format** vlan participation {untagged |tagged}< vlan id>

**Mode** Interface Config

##### 11.4.18.2 vlan protected

This command configures port protected property.

**Format** vlan protected {enable|disable}

**Mode** Interface Config

##### 11.4.18.3 vlan dropnq

This command configure port drop no 8021q frame .

**Format** vlan dropnq {enable|disable}

**Mode** Interface Config

##### 11.4.18.4 vlan pvid

This command configure port PVID.

**Format** vlan pvid <pvid>

**Mode** Interface Config

e.g. Switch(Interface 1)# vlan pvid 1

#### 11.4.19 Interface commands

This command change another interface

**Format** Interface <port number>

**Mode** Interface Config

e.g. Switch(Interface 1)# interface g1

## 11.4.20 PoE

### 11.4.20.1 func

This command configure poe function on a port

**Format** poe func {enable | disable}

**Mode** Interface Config

### 11.4.20.2 power-pri

This command configures the power priority on switch ports to decide which ports have priority to supply power which power devices are connected. Legal value are low, normal, middle or high priority. If the same power priority on the ports, the lower port index the higher power priority.

Low Set to low priority

Normal Set to normal priority

Middle Set to middle priority

High Set to high priority

**Format** poe power-pri level {low | normal | middle | high}

**Mode** Interface Config

### 11.4.20.3 detection

This command configures detection type on a port. set to 0,1,2,3,4 or 5

0 No Detection

1 Legacy Capacitive Detection only

2 IEEE 802.3af 4-Point Detection only (Default)

3 IEEE 802.3af 4-Point followed by Legacy

4 IEEE 802.3af 2-Point only

5 IEEE 802.3af 2-Point followed by Legacy

**Format** poe detection type {0 | 1 | 2 | 3 | 4 | 5}

**Mode** Interface Config

### 11.4.20.4 high-power

This command configures power Energy Mode on a port

on Start High Power (Support 30W power device)

off End High Power Mode (Support 15.4W power device)

**Format** poe high-power status {enable | disable}

**Mode** interface Config

## Appendix A: Basic Troubleshooting

In the unlikely event that the switch does not operate properly, follow the troubleshooting tips below. If more help is needed, contact Asante's technical support at [www.asante.com/support](http://www.asante.com/support).

Problem	Possible Solutions
The Power LED is not lit.	Check the power connection. Plug the power cord into another known working AC outlet.  The primary power supply has failed. Install the optional external power supply and have the primary power supply serviced as soon as possible.
The 10/100/1000 port Link LEDs are not lit.	Check the cable connections. Make sure the connectors are seated correctly in each port, and that the correct type of cable is used in each port. See <i>Chapter 2.6: Connecting to the Network</i> for more information.
The GBIC Link LED is not lit.	Check the GBIC connector. Make sure the cables are inserted correctly, with the Transmit (Tx) connector on one side of the link connected to the Receive (Rx) connector on the other side of the link.
Cannot establish communication to another device (switch, router, workstation, etc.).	<ul style="list-style-type: none"><li>• Make sure the Link LED for the port in use is on. Make sure the correct cable type is used. See <i>Chapter 2.6 Connecting to the Network</i> for more information on cabling procedures</li><li>• Make sure the IP address, subnet mask, and VLAN membership of the switch are correct</li><li>• Make sure the switch port and the device are both in the same VLAN</li><li>• Try to connect to a different port</li></ul>
Cannot auto-negotiate the port speed.	Make sure that auto-negotiation is supported and enabled on both sides of the link (in both devices).

## Appendix B: Specifications

### Ports

Fast Ethernet: 24 x 10/100BaseTX Fast Ethernet ports 12 x PSE ports, with Auto-Uplink: RJ-45 shielded connectors

Gigabit Ethernet: Ports 25 and 26 are combo. 2 x 10/100/1000BaseT Gigabit Ethernet ports with Auto-Uplink: RJ-45

shielded connectors. 2 x 1000BaseX Gigabit Ethernet ports: SFP Mini-GBIC

Console: Serial RS232: DB9 Male

### Status Indicators

Power: System is on (green)

Per 10/100 Port: Link (solid)/activity (blink) and PoE(amber)

Per Gigabit Port: Link (solid)/activity (blink), 1000 Mbps (amber)

### Performance

Efficiency: Wire-speed Gigabit switching (1,488,000 pps) and Fast Ethernet switching (148,800 pps)

Switch Architecture: Non-blocking 8.8 Gbps switch fabric

Flow Control: IEEE 802.3x flow control (full duplex) and back pressure (half-duplex)

Forwarding MAC Table: Up to 8K unicast addresses with automatic learning and aging

Packet Buffer: 256 KB

### L2+ Switching

Virtual LANs: IEEE 802.1q, 255 VLANs

Spanning Tree: IEEE 802.1d (STP), IEEE 802.1s (multiple), IEEE 802.1w (rapid reconfiguration), fast link

Flow Control: IEEE 802.3x

Link Aggregation: IEEE 802.3ad, LACP, up to 6 trunks

Authentication: IEEE 802.1x per port access control

Quality of Service: IEEE 802.1p, DiffServ and IP ToS

Power over Ethernet: Up to 15.4 watts per 10/100 port; 180 watts total

### Physical

Dimensions and Weight: 16.9 x 13.8 x 1.7 inches (430 x 350 x 44 mm) and 11.2 lb (5.1 Kg)

Mounting: Desktop or rack (rackmount kit included); 1U height

Operating Conditions: 32° to 104° F (0° to 40° C) with 10% to 90% non-condensing, relative humidity

Power: Internal universal switching, 100-240 VAC, 50/60 Hz, maximum 225 watts

### Standards Compliance

Network: IEEE 802.3 10BaseT, IEEE 802.3u 100BaseTX, IEEE 802.3ab 1000BaseT

IEEE 802.3z 1000BaseSX/LX, IEEE 802.3x full duplex flow control

Safety: UL

Emissions: FCC Class A

### Support

Technical Support: 24-hour support via web and ftp. 90-day email and telephone support

Product Warranty: 2-year product warranty covers defects in manufacturing and workmanship

# Appendix C: FCC Compliance and Warranty Statements

## C.1 FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

## C.2 Important Safety Instructions

**Caution: Do not use an RJ-11 (telephone) cable to connect network equipment.**

1. Read all of these instructions.
2. Save these instructions for later use.
3. Follow all warnings and instructions marked on the product.
4. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
5. Do not use this product near water.
6. Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.
7. The air vent should never be blocked (such as by placing the product on a bed, sofa or rug). This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
8. This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
9. This product is equipped with a three-wire grounding type plug, which is a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.
10. Do not allow anything to rest on the power cord. Do not place this product where people will walk on the cord.
11. If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
12. Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
13. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

### C.3 IntraCore Warranty Statement

Products: IntraCore IC3724PWR

Subject to the limitations and exclusions below, Asante warrants to the original end user purchaser that the covered products will be free from defects in title, materials and manufacturing workmanship for a period of three years from the date of purchase. This warranty excludes fans, power supplies, non-integrated software and accessories. Asante warrants that the fans and power supplies will be free from defects in title, materials and manufacturing workmanship for one year from date of purchase. Asante warrants that non-integrated software included with its products will be free from defects in title, materials, and workmanship for a period of 30 days from date of purchase, and the Company will support such software for the purpose for which it was intended for a period of 30 days from the date of purchase. This warranty expressly excludes problems arising due to compatibility with other vendors' products, or future compatibility due to third party software or driver updates.

To take advantage of this warranty, you must contact Asante for a return materials authorization (RMA) number. The RMA number must be clearly written on the outside of the returned package. Product must be sent to Asante postage paid. In the event of a defect, Asante will repair or replace defective product or components with new, refurbished or equivalent product or components as deemed appropriate by Asante. The foregoing is your sole remedy, and Asante's only obligation, with respect to any defect or non-conformity. Asante makes no warranty with respect to accessories (including but not limited to cables, brackets and fasteners) included with the covered product, nor to any discontinued product, i.e., product purchased more than thirty days after Asante has removed such product from its price list or discontinued shipments of such product.

This warranty is exclusive and is limited to the original end user purchaser only. Proof of purchase is required. This warranty shall not apply to secondhand products or to products that have been subjected to abuse, misuse, abnormal electrical or environmental conditions, or any condition other than what can be considered normal use.

ASANTE MAKES NO OTHER WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, REGARDING THE ASANTE PRODUCTS, EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, ALL WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. ASANTE'S LIABILITY ARISING FROM OR RELATING TO THE PURCHASE, USE OR INABILITY TO USE THE PRODUCTS IS LIMITED TO A REFUND OF THE PURCHASE PRICE PAID. IN NO EVENT WILL ASANTE BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES FOR THE BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, INCLUDING ECONOMIC LOSS, DAMAGE TO PROPERTY AND, TO THE EXTENT PERMITTED BY LAW, DAMAGES FOR PERSONAL INJURY, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE). THESE LIMITATIONS SHALL APPLY EVEN IF ASANTE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF THIS WARRANTY IS FOUND TO FAIL OF ITS ESSENTIAL PURPOSE.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or limitations on how long an implied warranty lasts, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from jurisdiction to jurisdiction.

## Index

Cabling		VLAN .....	71
console .....	20	weighted fair queuing .....	57
Ethernet .....	18	Connecting	
procedures .....	17	console .....	13, 20
CLI		network .....	17
advanced features .....	29	PC .....	22
global configuration mode .....	27	power .....	17
history .....	31	Console	
interface configuration mode .....	28	baud rate .....	21
privileged top mode .....	25	interface .....	13
top user mode .....	24	Default	
understanding .....	24	IP address .....	64
Command		password .....	13
configuration .....	27	port-priority .....	45
ethernet interface .....	28	SNMP trap authentication .....	89
help .....	30	SNMP write community .....	89
history .....	31	spanning-tree .....	74, 75
IGMP .....	49	Description .....	11
interface .....	28	front panel .....	11
Configuring		Features .....	7
Ethernet .....	28	GUI	
IGMP .....	48	front panel screen .....	63
interface .....	28	general information screen .....	64
priority queuing .....	58	SNMP configuration .....	89
Quality of Service .....	57	software version .....	64
rate limit .....	60	VLAN configuration .....	71
SNMP Configuration, GUI .....	89	Help	
traffic shaping interface .....	60		



context sensitive .....	30	weighted fair queuing .....	57
<b>IGMP</b>		<b>Rapid Spanning-Tree</b>	
configuration .....	48	edge port .....	43
host-query .....	49, 79	link type .....	43
overview .....	48	port path cost.....	44
<b>Installation</b>		port priority.....	44
hardware .....	14, 34, 109	<b>Rate Limit</b>	
into rack.....	15	configuring.....	60
mini GBIC .....	16	examples .....	60
<b>IP</b>		<b>Requirements</b>	
assign addresses.....	64	airflow .....	15
configuration .....	64	environment.....	15
multicast configuration.....	48	power.....	15
range .....	64	tools.....	15
<b>Managing</b>		<b>Safety</b>	
front panel screen.....	63	guidelines .....	14
general information screen .....	64	<b>Security</b>	
information screen .....	63	SNMPv3 .....	89
IP multicast .....	48	<b>SNMP</b>	
<b>Password</b>		traps .....	89
default.....	13	<b>Spanning-Tree</b>	
<b>Priority Queuing</b>		default.....	45
configuring .....	58	<b>Traffic Shaping</b>	
examples .....	59	overview .....	60
monitoring.....	59	<b>Troubleshooting</b> .....	138
<b>Quality of Service</b>		<b>VLAN</b>	
configuration .....	57	configuration, GUI.....	71
priority queuing.....	58	trunk .....	55
traffic shaping .....	60	<b>Weighted Fair Queuing</b>	

bandwidth .....57  
configuration .....57

monitoring.....57, 58, 59, 60